RICERCHE

FRODI INFORMATICHE E CARTE DI CREDITO MAGNETICHE. UN'ANALISI DEL *CREDIT CARD FRAUD ACT*

SOMMARIO

I. CONSIDERAZIONI INTRODUTTIVE.

1. PREMESSA.

Il giurista non può ignorare che i nuovi fenomeni, che si presentano nella realtà quotidiana, gli impongono un ripensamento ed una valutazione di adeguatezza dell'ordinamento giuridico rispetto a tali situazioni[1]. Ciò vale in particolare per il diritto penale, i cui principi informatori, sia nei paesi di *common law* sia in quelli di *civil law*, sono ispirati a criteri di stretta legalità (*nullum crimen, nulla poena sine lege*) ed al divieto di ricorso all'analogia[2] che ne limitano la possibilità di adeguamento. In altri settori esistono infatti alcuni correttori interni od esterni al sistema, come nel diritto civile il ricorso all'analogia in funzione integrativa o all'autonomia privata[3].

È già stato rilevato come l'approccio comparatistico con il diritto statunitense

[1] Si rimanda alle opere di carattere generale: M.G. LOSANO, *Informatica per le scienze sociali*, Einaudi, Torino, 1985; ID., *Il diritto privato dell'informatica*, Einaudi, Torino, 1986, e ID., *Il diritto pubblico dell'informatica, idem*, che contengono un'ampia bibliografia anche internazionale; Rodolfo PAGANO, *Informatica e diritto*, Giuffrè, Milano, 1986; Vittorio FROSINI, *Il diritto nella civiltà tecnologica*, Giuffrè, Milano, 1981; Ettore GIANNANTONIO, *Introduzione all'informatica giuridica*, Giuffrè, Milano, 1984.

[2] Si veda a questo proposito CHERIF M. BASSIOUNI, *Diritto penale degli Stati Uniti d'America*, Giuffrè, Milano, 1985, p. 66 ss.; G. CORRIAS LUCENTE, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Il Diritto dell'informazione e dell'informatica* (di seguito citata per motivi di brevità come DII), 1987, p. 168; Carlo SARZANA, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1984, p. 22; Alessandro TRAVERSI, *Il diritto dell'informatica*, Ipsoa, Milano, 1985, p. 192; Lorenzo PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, *DII*, 1985, p. 951; Ettore GIANNANTONIO, *op. cit.*, p. 278.

[3] In tal senso anche G. CORRIAS LUCENTE, *op. cit.*, p. 168. Negli Stati Uniti l'ordinamento giuridico è anche caratterizzato dalla « mancanza di tipicità delle fonti di obbligazione e dei fatti di autonomia privata e dalla possibilità per il giudice di riconoscere forza obbligatoria a tutti quegli atti e fatti dell'autonomia privata

sia particolarmente interessante[4] in ordine allo studio dei reati informatici[5] per diversi motivi. In primo luogo perché la società statunitense è ad un livello tecnologico superiore al nostro. Secondariamente il legislatore di quel paese, come nel caso della legge in esame, per ragioni che sono proprie degli ordinamenti di *common law*[6], ha già dato concreta attuazione ad alcune esigenze emerse nel paese emanando apposite norme in questo settore. All'utile esame dell'esperienza compiuta negli Stati Uniti occorre aggiungere anche il rischio che l'utilizzo di reti telematiche internazionali sempre più complesse renda possibili i c.d. « paradisi informatici »[7].

2. Le carte di credito negli Stati Uniti.

La carta di credito, che può vantare origini storiche antiche[8], ha avuto solo negli ultimi decenni un rapido e crescente sviluppo, soprattutto negli Stati Uniti[9].

Gli aspetti socio-economici di tale fenomeno esulano dalle finalità del presente lavoro. È comunque opportuno fornire, al lettore italiano, due soli dati che sintetizzano l'estensione ed importanza assunte negli U.S.A. dalle carte di credito. Nel 1983 ne circolavano complessivamente in quel paese 577 milioni (equivalenti all'80% del totale mondiale) che rappresentavano un giro d'affari tra i 60 e i 70 miliardi di dollari, pari al 30-35% degli acquisti effettuati in tutti gli Stati Uniti[10].

Le ragioni di questa diffusione sono legate all'incapacità dell'assegno di far fronte alle sempre maggiori esigenze della nostra società. I limiti geografici e spesso fiduciari collegati alla circolazione degli assegni, l'aumento della loro falsificazione e dei costi di gestione da parte degli istituti finanziari ne hanno decretato il superamento[11].

3. Informatica e carte di credito.

La carta di credito, così come era apparsa negli anni '50 e commercializzata nei due decenni successivi, non era però riuscita ad introdursi in alcuni importanti segmenti di mercato.

Gli istituti finanziari decisero, verso la fine degli anni '70, di studiare e lanciare sul mercato un nuovo strumento di pagamento che costituisse una valida

---

che la realtà sociale già considera vincolanti ». E. Giannantonio, *Trasferimenti elettronici di fondi e autonomia privata*, Giuffrè, Milano, 1986, p. 17.

[4] Si veda Guido Alpa, *I contratti di utilizzazione dei computers*, in *Informatica e diritto*, Le Monnier, Firenze, 1983, p. 33; Id., *Il diritto dei computers*, *DII*, 1985, p. 55; e da ultimo tali ragioni sono ben evidenziate in G. Corrias Lucente, *op. cit.*, p. 172 ss.

[5] Si preferisce questa espressione come traduzione di *computer-related crimes* (termine più appropriato di *computer crimes*) a quella più riduttiva di reati elettronici. L'elettronica costituisce infatti una delle modalità tecniche per la gestione delle informazioni. Ma vi sono altre tecniche, magnetiche, chimiche, ottiche, via satellite attualmente in uso. In tal senso si veda Antonio Ruberti, *Tecnologia domani*, Laterza-Seat, Bari, 1985, p. X, C. Sarzana, *op. cit.*, p. 21; L. Picotti, *op. cit.*, p. 939 ss.; G. Corrias Lucente, *op. cit.*, p. 171 ss.; *contra*: Lucia Tria, *Osservazioni in tema di reati elettronici*, in *Arch. pen.*, 1984, p. 283. Col termine « reati informatici » si comprendono generalmente non solo i reati in senso stretto ma anche quei fatti meritevoli di tutela penale. Si veda al riguardo Klaus Tiedemann, *Criminalità da computer*, in *Politica del diritto*, 1984, p. 613 ss. e G. Corrias Lucente, *op. cit.*, p. 172.

[6] La maggiore elasticità del legislatore e l'importanza del precedente giurisprudenziale, interpretato in maniera restrittiva in modo da limitarne al massimo gli effetti sul *common law*. Si veda Mario G. Losano, *I grandi sistemi giuridici*, Einaudi, Torino, 1978, pp. 125 e 141.

[7] M.G. Losano, *Informatica*, cit., p. 224 ss. e Id., *Il diritto pubblico*, cit., p. 11.

[8] Per una ricostruzione storica di tale sviluppo si veda Henry Hauser-Augustin Renaudet, *L'età del Rinascimento e della Riforma*, Einaudi, Torino, 2ª ed., 1970, p. 400 ss.; Henry Pirenne, *Storia d'Europa dalle invasioni barbariche al XVI secolo*, Sansoni, Firenze, 1956, p. 141 ss.; Mario Giuliano, *La cooperazione degli stati e il commercio internazionale*, Giuffrè, Milano, 4ª ed., 1978, p. 230 ss.; Carlo Di Nanni, *Pagamento e sostituzione nella carta di credito*, Jovene, Napoli, 1983, p. 25 ss.

[9] Lewis Mandell-Neil Murphy, *Bank Cards*, American Bankers Association, 1977, p. 4 ss.; Tony Drury-Charles Ferrier, *Credit Cards*, Butterworths, London, 1984, p. 4 ss.; AA.VV., *Bank Cards-Seminar*, American Bankers Association, Washington, 1980; C. Di Nanni, *op. cit.*, p. 7 e p. 41 ss.

[10] Sugli aspetti socio-economici di tale fenomeno si vedano gli autori americani della nota precedente nonché James Martin-Adrian Norman, *The Computerized Society-An appraisal of the impact of computers on society over the next fifteen years*, Prentice Hall, Englewood Cliffs, N.J., 1970 (che preconizza la cashless/checkless society); August Bequai, *The Cashless Society: EFT at the Crossroads*, J. Wiley & Sons, New York, 1980, p. 8 ss.; E. Giannantonio, *op. ult. cit.*, p. 8 (i cui dati non sono peraltro recenti) e le due relazioni presentate al Congresso dall'*American Bankers Association* e dal Dipartimento del Tesoro, *Hearings before the House of Representatives, Subcommittee on Crime*, in *Judiciary Committee*, ABS, 1985, H521-39 rispettivamente a p. 19 e p. 151. D'ora in avanti queste audizioni tenute presso la Camera dei Rappresentanti saranno citate per brevità come *Hearings*.

[11] L. Mandell-N. Murphy, *op. cit.*, p. 6 ss.; T. Drury-C. Ferrier, *op. cit.*, p. 20 ss.; A. Bequai, *op. cit.*, p. 8 ss.; Richard Shriver, Dipartimento del Tesoro, *Hearings*, p. 151; C. Di Nanni, *op. cit.*, p. 41 ss.

alternativa alla carta di credito tradizionale. L'obiettivo era la realizzazione di un nuovo strumento di pagamento che, aumentando i benefici per il cliente e per l'istituto emittente[12], facesse presa anche presso una nuova fascia di clientela. L'utilizzo delle tecnologie informatiche[13], su cui il settore bancario aveva compiuto scelte strategiche ed investimenti produttivi per il futuro destinati a divenire irreversibili[14], divenne così una scelta obbligata.

D'altra parte un imprevisto incentivo alla realizzazione di questo progetto era venuto dalla necessità di far fronte all'enorme mole di frodi perpetrate a partire dal 1979 mediante le carte di credito[15].

Nasce così la carta di credito magnetica (*debit card*) che può essere usata in connessione con i terminali elettronici dell'istituto finanziario o della società commerciale emittente[16].

I primi collegamenti in rete si realizzarono tra l'elaboratore centrale di un istituto finanziario e i terminali periferici dello stesso istituto. Da questa limitata possibilità si è passati, grazie ad accordi interbancari, ad una vera e propria rete telematica complessa[17], nella quale la stessa carta magnetica può essere utilizzata anche presso « sportelli bancari automatici » (o ATMs) di istituti finanziari diversi situati in zone lontane dall'istituto emittente la carta. Un ulteriore progresso è l'utilizzo di tali carte anche su terminali installati presso grandi magazzini ed esercenti privati (terminali punto di vendita o POSs)[18].

L'ultimo progetto in questo settore, ancora in fase di studio e sperimentazione, consiste nella produzione di una vera e propria carta informatica che, non discostandosi per caratteristiche fisiche dalla carta ora in circolazione, avrà incorporato un minuscolo microprocessore che la renderà in grado di diventare « intelligente »[19].

4. Il *Credit Card Fraud Act of 1984*.

Il presente studio ha per oggetto il *Credit Card Fraud Act of 1984*, la legge penale federale degli Stati Uniti emanata nell'ottobre 1984 dal Congresso[20] per reprimere le frodi compiute con carte di credito.

La natura del presente lavoro è quindi prevalentemente penalistica ed avrà come primario riferimento il diritto statunitense, pur non tralasciando alcuni cenni civilistici. Saranno inoltre effettuate alcune comparazioni con il diritto italiano.

Questa legge comprende tutti i tipi di carte di credito ma, per le finalità di questo studio, saranno esaminate esclusivamente[21] le carte di credito informatiche[22], cioè quelle che abilitano l'utente

[12] Per l'istituto di credito il contenimento dei costi del personale e l'eliminazione della franchigia di addebito in conto (in alcuni casi pari a 45/60 gg. di valuta); per il cliente la possibilità di utilizzare tale strumento di pagamento 24 ore al giorno ed in qualsiasi località. Si veda L. Mandell-N. Murphy, *op. cit.*, p. 25 ss. ed Henry Berry, *Bank Cards-Seminar*, cit., p. 122 ss.

[13] Per una storia dell'informatica si veda Mario G. Losano, *Informatica per le scienze sociali*, cit., p. 143 ss. dov'è ben analizzato il miglioramento delle prestazioni degli elaboratori sia in termini di facilità di gestione che di costi per l'utente.

[14] Clifford L. Karchmer, Battelle Memorial Institute, *Hearings*, p. 314; si vedano inoltre gli autori americani citati alla nota n. 9.

[15] Tale necessità divenne in seguito prioritaria. Le frodi rappresentarono una perdita per gli istituti finanziari (e di conseguenza un aumento di costi per l'utenza) di 95 milioni di dollari nel 1981 e di 128 milioni nel 1982. Nello stesso anno le rapine ai danni d'istituti finanziari ammontarono a 46,8 milioni. Si veda William D. Neumann della *Visa*, Thomas Kelleher della *Mastercard*, Stephen Weinstein dell'*American Express*, *Hearings*, rispettivamente a pp. 76, 96 e 278 ss.

[16] Sulle caratteristiche fisiche e magnetiche delle carte si veda H. Berry, *op. cit.*, p. 106 ss.; A. Bequai, *op. cit.*, p. 34 ss.; Michael Housemann, *Bank Cards-Seminar*, cit., p. 67 ss.; T. Drury-C. Ferrier, *op. cit.*, p. 16.

[17] Si veda in proposito M. Losano, *op. ult. cit.*, p. 224 ss.

[18] Sugli ATMs e POSs si vedano gli autori citati alla nota n. 9 ed inoltre A. Bequai, *op. cit.*, p. 4 ss.; Id., *Technocrimes*, p. 145 ss. ed i seguenti autori italiani, L. Tria, *op. cit.*, p. 282 ss.; E. Giannantonio, *op. ult. cit.*, p. 4 ss.; Pietro Nuvolone, *La trasmissione elettronica dei fondi e la tutela dell'utente*, *DII*, 1985, p. 594 ss.

[19] Si tratta della « carta intelligente » o *smart card*. Si veda T. Kelleher, S. Weinstein e Henry Dreifus, *Hearings*, p. 142, 281 e 260 rispettivamente. In Italia i primi passi di tale carta sono descritti da E. Giannantonio, *op. ult. cit.*, p. 14.

[20] *Title 18 United States Code section 1029 - Public Law 98-473 Oct. 12, 1984 - 98 Statutes at Large 2183.*

[21] È peraltro evidente che tale trattazione avrà molti punti in comune con le altre carte di credito proprio per le finalità generali che il legislatore si è proposto.

[22] Si preferisce usare il termine carte informatiche a quello più riduttivo di carte magnetiche per due ragioni. La prima per potervi ricomprendere, al di là dei materiali concretamente usati anche i futuri cambiamenti tecnologici (si veda ad es. la *smart card* di cui alla nota n. 19). Tale preoccupazione è stata fatta propria anche dal legislatore statunitense che ha usato l'espressione « strumenti di accesso » su cui si veda oltre al paragrafo 4. La seconda perché « lo "specifico" delle nuove tecnologie è altro, è immateriale in una certa misura ». Si veda a tale proposito A. Ruberti, *op. cit.*, p. X.

all'utilizzo di un terminale elettronico per compiervi trasferimenti elettronici di fondi.

È opportuno a questo punto sottolineare come l'iter legislativo del *Credit Card Fraud Act*, voluto e sostenuto da diverse *lobbies*[23] rappresentanti gli interessi degli istituti emittenti (*Visa, Master card, American Express* e *American Bankers Association*), del mondo politico, giuridico, industriale e culturale, sia stato relativamente lungo e complesso[24], ma estremamente interessante per l'approfondimento degli aspetti informatici e giuridici.

Nei lavori parlamentari che l'hanno preceduta, questa legge è stata infatti discussa ed esaminata insieme a quella relativa all'accesso abusivo o non autorizzato agli elaboratori. Il Congresso le ha poi approvate congiuntamente[25]. Infatti le carte informatiche avevano in comune con questa seconda legge il problema della definizione dell'accesso abusivo o non autorizzato ad un terminale elettronico. I parlamentari hanno quindi avuto modo — nel corso di diverse sedute la cui documentazione è di circa mille pagine — di ascoltare oltre 40 autorevoli e competenti personalità, che hanno posto l'accento sui più importanti aspetti finanziari, giuridici, informatici e culturali di queste frodi.

II. Profili civilistici delle carte informatiche.

1. La legislazione negli U.S.A.

Le carte di credito costituiscono un fenomeno complesso, comprendente un insieme di fattispecie diverse, caratterizzate ciascuna da funzioni proprie e riconducibili ad un quadro unitario e sistematico[26], in funzione di una delle finalità realizzate da ciascuna di esse. Si tratta dell'adempimento, con modalità e rapporti intersoggettivi diversificati, di un pagamento.

La carta informatica che possiamo definire come lo strumento che abilita l'utente all'utilizzo di un terminale elettronico per compiervi trasferimenti elettronici di fondi, solo in una visione riduttiva può essere concepita come un sofisticato strumento di mero pagamento. In realtà questa carta permette al titolare di compiere, oltre all'importantissima funzione di pagamento, diverse altre operazioni, quali quelle di controllo del conto, di prelievo e deposito di denaro sul proprio conto e di accesso ad altre informazioni finanziarie in senso lato[27].

Negli Stati Uniti sotto il profilo giuridico esiste una specifica disciplina legale che stabilisce, a tutela del consumatore, precisi obblighi e responsabilità ed informa a tali criteri la disciplina contrattuale tra le parti relativa a questi trasferimenti[28].

---

[23] Per una ricostruzione del diritto costituzionale degli Stati Uniti e l'importanza ivi assunta dalle *lobbies*: Guglielmo Negri, *Il diritto costituzionale degli Stati Uniti*, Nistri-Lischi, Pisa, 1960, p. 262; Lawrence Friedman, *American Law*, W.W. Norton & Co., New York, London, 1984, p. 362.

[24] La prima proposta di legge, presentata alla Camera dei Deputati l'1 giugno 1983 col nome di *Credit Card Counterfeiting and Fraud Act of 1983* (H.R. 3181), riguardava solamente le carte di credito mentre la seconda, presentata alla Camera il 14 luglio 1983 col nome *Counterfeit Access Device and Computer Fraud Act of 1983* (H.R. 3570), aveva il più ambizioso intento di reprimere non solo alcuni illeciti comportamenti posti in essere mediante carte di credito ma anche altri posti in essere con un elaboratore. Quasi contemporaneamente (21 settembre 1983) al Senato veniva presentato il *Credit and Debit Card Counterfeiting and Fraud Act of 1983* (S. 1870). Questo *bill*, riguardante le sole carte di credito, ebbe un proprio *iter* ma non fu approvato.

Gli altri due furono esaminati insieme in due lunghe sedute parlamentari che misero in evidenza la necessità di un nuovo *bill* che separasse i due argomenti. Esso fu presentato il 13 marzo 1984 col nome di *Counterfeit Access Device and Computer Fraud and Abuse Act of 1984* (H.R. 5112). La versione definitiva fu però compilata dalla Sottocommissione per il crimine della Commissione Giustizia il 24 luglio 1984 (H.R. 5616).

Contemporaneamente venivano presentati altri *bills* per la modifica del *Truth in Lending Act* relativo alle carte di credito tradizionali, che vennero discussi ma non approvati.

[25] Il *Counterfeit Access Device and Computer Fraud and Abuse Act of 1984* modifica sia il paragrafo 1029 (*Fraud and related activity in connection with access device*) che il 1030 (*Fraud and related activity in connection with computers*) del capitolo 47 - titolo 18 U.S.C. Si veda con particolare riferimento alla seconda legge il brillante lavoro di G. Corrias Lucente, *op. cit.*, p. 167 ss. e p. 519 ss.

[26] M. Hosemann, *op. cit.*, p. 65 ss.; H. Berry, *Ivi*, p. 106; Floyd I. Clarke, Dipartimento di Giustizia, *Hearings*, p. 163; Aldo Angelo Dolmetta, *La carta di credito*, Giuffrè, Milano, 1982, p. 2 ss.; C. Di Nanni, *op. cit.*, p. 14.

[27] Si vedano i testi citati alla nota n. 11.

[28] Si tratta dell'*Electronic Fund Transfers Act* (chiamato anche EFTA) la cui approvazione è stata preceduta da appositi studi socio-economici per valutarne l'impatto sulla società americana. Il testo di legge e la *Regulation E* è reperibile in *Computer Law Journal* (di seguito CLJ), 1980, n. 1, p. 232 ss. Per un commento giuridico si veda Melvin Katskee & Ann Wright, *An Overview of the Legal Issues Confronting the Establisment of Electronic Funds Transfer Services CLJ*, 1980, vol. II, n. 1, pp.

Sotto il profilo tecnico i trasferimenti di fondi negli U.S.A. sono gestiti da una rete interbancaria che agisce con modalità *on-line* in modo cioè che ogni operazione avvenga in tempo reale. È quindi difficile ipotizzare cancellazioni di operazioni (ad eccezione di quelle pre-autorizzate), anche se si può verificare qualche ipotesi di questo tipo. Particolare importanza assume anche nell'ambito delle carte informatiche la predisposizione di appropriate misure di protezione di tipo fisico e logico per impedire il compimento di illeciti[29]. Sono esempio delle prime la collocazione dei terminali in appositi locali[30], delle seconde il codice d'identificazione personale (detto, negli U.S.A., PIN: *personal identification number*), l'accesso ad un numero di funzioni specifiche, nonché i vari limiti giornalieri o mensili stabiliti per ciascuna operazione ed altre ancora[31].

Da un punto di vista giuridico per « trasferimenti elettronici di fondi s'intende qualsiasi trasferimento di fondi, purché non avviato con un assegno bancario, un assegno circolare o simili strumenti cartacei, iniziato tramite un terminale elettronico, un telefono, un *computer* o una banda magnetica, avente per scopo l'ordine, l'istruzione o l'autorizzazione ad un istituto di credito di addebitare od accreditare un conto. Il termine comprende, pur senza esaurirsi con essi, i POSs, gli ATMs, i versamenti o prelevamenti diretti di fondi e i trasferimenti iniziati mediante telefono »[32].

La disciplina legale e contrattuale così accennata stabilisce la responsabilità degli istituti di credito per l'inadempimento degli ordini di trasferimento e i casi in cui è responsabile il cliente o l'istituto di credito in caso di trasferimento non autorizzato[33].

In particolare, qualora il contratto di trasferimento elettronico di fondi non venga adempiuto (sia nel caso in cui l'istituto finanziario per errore abbia addebitato sul conto di un altro cliente una somma non dovuta, sia nel caso che l'istituto non abbia eseguito l'ordine di trasferimento richiestogli) sorge a carico dello stesso una responsabilità contrattuale. Essa comprende tutti i danni diretti ed immediati causati al contraente dall'ingiustificata inosservanza di un ordine autorizzato ed anche i danni indiretti, qualora sussista il dolo[34].

Non sussiste responsabilità dell'istituto nel caso di mancanza di fondi adeguati o perché soggetti a pignoramento o altro vincolo o nel caso in cui l'ordine, se eseguito, avrebbe violato i limiti del credito. Altra esclusione di responsabilità si ha nell'ipotesi di caso fortuito o forza maggiore o guasto tecnico noto al contraente nel momento in cui ha disposto l'ordine di trasferimento. In caso di guasto tecnico l'ordine è sospeso fino al ripristino del sistema elettronico, fatta salva la possibilità per il creditore di essere pagato con mezzo diverso[35].

È chiaro come questa disciplina, stabilendo precise responsabilità, sia un valido contributo alla certezza del diritto.

Non manca tuttavia qualche ombra anche in questa legge. L'utente può essere risarcito solo del danno attuale e provato, se il mancato *facere* dell'istituto finanziario fu non intenzionale ed esso agì ragionevolmente per prevenire l'errore. Se questo ente commise un errore in « buona fede », diverso dalla negligenza o dall'atto non intenzionale, esso è responsabile, ma la responsabilità è limitata. Il *Federal Reserve Board*, al quale è stato demandato l'emanazione delle disposizioni applicative della legge, si è finora rifiutato di emanare qual-

---

7-26; James Brown, *Implications of the Informational Nature of Payments*, *ivi*, pp. 153-166; E. GIANNANTONIO, *op. cit.*, p. 21 ss.; L. TRIA, *op. cit.*, p. 284 ss.

[29] Per un più dettagliato esame generale di tali protezioni si veda Gian Maria CASTELLI, *Il dolo informatico*, F. Angeli, Milano, 1986, p. 37 ss.; Ferdinando MAZZEI, *Sicurezza e riservatezza delle informazioni negli enti e nelle imprese*, *ivi*, 1983, p. 60 ss.; A. TRAVERSI, *op. cit.*, p. 188 ss.

[30] In un primo tempo fu data scarsa importanza a questo tipo di protezione. Si veda A. BEQUAI, *opp. citt. passim*.

[31] In particolare sulle protezioni relative alle carte informatiche si veda Fred M. GREGURAS & David J. SYKES, *Authentication in EFT: the Legal Standard and the Operational Reality*, *CLJ*, 1980, vol. II, n. 1, pp. 67-86; H. DRYFUS, *Hearings*, p. 264; S. WEINSTEIN, *Hearings*, p. 280. Il superamento di tali difese ha reso necessario la stipulazione di apposite polizze assicurative e di moderne metodologie di EDP *auditing*. Si veda al riguardo M.G. LOSANO, *Il diritto privato*, cit., p. 144 e Francesco STORACE, *La copertura del rischio informatico*, *DII*, 1986, p. 652 ss. e G.M. CASTELLI, *op. cit.*, p. 67 ss.

[32] Si veda la *Regulation E section 205.2*; L. TRIA, *op. cit.*, p. 283 ed E. GIANNANTONIO, *op. cit.*, p. 7 che distingue due definizioni di trasferimento elettronico di fondi.

[33] Si veda la nota n. 28.

[34] In questo senso F. GREGURAS-D. SYKES, *op. cit.*, pp. 67-86.

[35] EFTA sec. 912.

siasi *regulation* riguardo a questo punto per chiarire gli *standard* di responsabilità assegnati. Il FRB suggerisce che gli istituti finanziari limitino contrattualmente la loro responsabilità per questo tipo di rischio. In questo modo, dato che il proposito della legge è di protezione del consumatore, non è chiaro quali siano i limiti di responsabilità che possano essere stabiliti senza con ciò negare il proposito perseguito dalla legge[36].

I trasferimenti non autorizzati sono così definiti: « trasferimenti elettronici di fondi dal conto di un cliente, disposti da persona diversa dal cliente stesso e senza mandato, qualora da tale trasferimento il cliente non riceva alcun beneficio »[37]. La responsabilità è ripartita tra cliente ed istituto finanziario in funzione del principio di colpa, in modo da imporre al primo un comportamento diligente ed al secondo la predisposizione dei mezzi idonei a rendere sicuri ed affidabili i trasferimenti. Il cliente è sempre responsabile fino all'ammontare di 50 dollari. Nel caso invece che egli non usi la necessaria diligenza e non avvisi l'istituto di credito entro due giorni lavorativi dallo smarrimento o dal furto della carta, la sua responsabilità raggiunge l'importo di 500 dollari. Infine, se non rileva trasferimenti non autorizzati od errori nell'estratto conto trasmessogli periodicamente dall'istituto entro 60 giorni dall'invio, la sua responsabilità diventa illimitata[38].

Questa disciplina non esaurisce tutti i problemi giuridici connessi con questi trasferimenti di fondi. Si tratta infatti di operazioni che, pur accomunate dal fatto di essere effettuate in modo informatico, sono a volte anche molte diverse tra loro. Un altro grave problema è la difficoltà per l'utente di dimostrare all'istituto finanziario la mancata o parziale erogazione del contante da parte di un ATM o l'erroneo addebito in conto di un trasferimento non autorizzato[39].

Occorre infine notare come l'ordine di trasferimento elettronico o *draw order* (che peraltro non costituisce ancora adempimento nei confronti del terzo creditore, secondo la legislazione statunitense) sia soggetto al *common law*, mentre i trasferimenti elettronici veri e propri (*pay orders*) sono disciplinati dall'*Electronic Fund Transfer Act* e l'obbligazione assunta dall'istituto di credito non è quella di trasferire l'ordine ma di dar corso all'effettivo pagamento. Autorevole dottrina, nota « l'emergere dell'autonomia dell'ordine di pagamento »[40] che, una volta eseguito, diventa indipendente dal rapporto giuridico sottostante e può essere fatto valere in modo autonomo.

2. (SEGUE) E IN ITALIA.

In Italia la diffusione e le possibilità di utilizzo dei terminali elettronici che abilitano l'accesso delle carte informatiche è abbastanza arretrata rispetto agli S.U. In particolare, gli « sportelli automatici » Bancomat non sono abilitati ad effettuare tutte le operazioni realizzabili dagli ATMs. Infatti « Il Servizio Bancomat consente al Correntista di prelevare contante a valere sul suo conto corrente presso... » (art. 1, comma 1 Norme che regolano il Servizio Bancomat)[41], mentre i già reclamizzati omologhi dei POSs sono ad uno stadio ancora di sperimentazione presso alcuni grossi supermercati (Standa, GS, Coin, Euromercato, Rinascente)[42].

A questi limiti di fatto va ad aggiungersi una duplice carenza: giuridica, per l'inesistenza di una specifica legislazione analoga a quella emanata negli U.S.A., e tecnica, poiché la rete interbancaria, con qualche eccezione come la Cassa di Risparmio delle Provincie Lombarde e la Banca Nazionale del Lavoro, non

---

36 Si veda la nota 34.

37 EFTA sec. 903 n. 11.

38 EFTA sec. 908 e P. NUVOLONE, *op. cit.*, p. 594; E. GIANNANTONIO, *op. cit.*, p. 32.

39 Si veda come tali problemi siano presenti, fin dall'emanazione della legge, nei giuristi più attenti Theresa A. EINHORN, *Terminal based EFT Services: the Need for Uniform Federal Legislation, CLJ*, 1980, vol. II, n. 1, pp. 31-47; Mark BUDNITZ, *Problems of Proof When there's a Computer Goof: Consumer Versus ATMs, ivi*, pp. 49-65 e James VERGARI, *Electronic Giro for the United States, ivi*, pp. 101-113. Nello stesso volume vi sono inoltre altri saggi sulle implicazioni sociali ed economiche degli EFT.

40 E. GIANNANTONIO, *op. cit.*, p. 34 ss.

41 Le norme che regolano il Servizio Bancomat sono riprodotte in allegato all'articolo di Gian Luca BRANCADORO, *Profili di responsabilità contrattuale ed aquiliana della banca nell'erogazione del servizio Bancomat, DII*, 1985, p. 660.

42 Si veda l'elenco delle operazioni effettuabili dagli ATMs italiani e maggiori dettagli sui POSs italiani in E. GIANNANTONIO, *op. cit.*, pp. 3 e 11 ss.

opera ancora appieno in termini di collegamenti *on-line*[43].

Le limitazioni sopra delineate vengono ulteriormente aggravate dalla disciplina contrattuale predisposta dagli istituti di credito, ed evidentemente stabilita a tutela dei loro interessi, che prevede l'accessorietà del servizio Bancomat rispetto ad un conto corrente già istituito (artt. 1-4-10-12 Norme che regolano il Servizio Bancomat). È pertanto evidente, per la natura accessoria di tali pattuizioni, che il venir meno del contratto principale fa venir meno anche queste disposizioni accessorie.

Si osservino inoltre le seguenti disposizioni: « al fine di tutelare il buon funzionamento e di garantire la sicurezza del Servizio Bancomat, l'Azienda di credito ha facoltà, in qualunque momento, per motivi di sicurezza, di procedere al blocco della Carta anche senza necessità di preventivo avviso al Correntista » (art. 4, comma 4). L'Azienda di credito ha inoltre la facoltà « di modificare l'ubicazione degli Sportelli Bancomat, sospendere o abolire il servizio in qualunque momento, senza assumere responsabilità per eventuali temporanee interruzioni del servizio medesimo, anche se non comunicate al Correntista » (art. 3, comma 2), « di recedere dal presente contratto in qualunque momento dandone comunicazione scritta al Correntista... » (art. 9, comma 1). Ancora « nel caso di utilizzo errato rispetto alle istruzioni previste dal ..., o comunque difformi dalle presenti disposizioni, lo Sportello Bancomat, per motivi di sicurezza, trattiene la Carta » (art. 14, comma 3)[44]. È stato giustamente rilevato come queste disposizioni, se applicate negli U.S.A. non sarebbero considerate valide in base ai principi stabiliti nell'EFTA[45].

Dall'insieme delle norme che regolano il servizio Bancomat emerge che, relativamente all'adempimento di questo contratto, il cliente non è in un alcun modo tutelato: infatti esso « non determina profili di responsabilità né in capo alla Banca contraente per l'operato delle altre banche aderenti, né in capo a queste ultime, per il loro operato, nei confronti del correntista »[46]. Quindi nessun obbligo per la banca di soddisfare le richieste di prelievo dell'utenza ed, in aggiunta, anche la possibilità di « sospendere o abolire il servizio in qualunque momento, senza assumere responsabilità per eventuali temporanee interruzioni del servizio, anche se non comunicate al correntista » (art. 3, comma 2). Inoltre « in base al contratto, il correntista non può far valere alcuna eccezione in ordine all'esattezza della somma erogata dall'impianto »[47].

Per quanto riguarda i trasferimenti non autorizzati, la particolarità tecnica del sistema *off-line* rende possibili abusi sia da parte del correntista, sia di terzi estranei al titolare della carta.

La prima ipotesi dà vita ad una situazione anomala dal punto di vista giuridico che sarà esaminata nell'ultimo paragrafo di questo lavoro.

In caso di trasferimenti non autorizzati compiuti da terzi, l'utente è responsabile sia nei casi di smarrimento o sottrazione della carta non denunciati nelle forme previste, sia nei casi di smarrimento o sottrazione della carta prima che sia trascorso il tempo ragionevolmente necessario, peraltro non specificato, perché la banca blocchi la carta, sia nei casi in cui vi sia stato abuso o illecito uso della carta non derivanti da smarrimento o sottrazione[48].

3. Natura giuridica della carta informatica.

È impresa difficile cercare definizioni giuridiche appropriate nell'ambito di un sistema di *common law* in cui i giuristi non hanno consuetudine alla formulazione di concetti generali ed astratti,

[43] Il collegamento *off-line* non opera in tempo reale e non sarebbe quindi un trasferimento elettronico di fondi vero e proprio. Tale sistema è inoltre un facile bersaglio per la criminalità informatica. « Di conseguenza mancherebbe in Italia qualsiasi norma, sia essa di carattere statale sia essa di carattere privato, in tema di trasferimenti elettronici... ». E. Giannantonio, *op. cit.*, p. 42. Pare comunque che il passaggio al sistema *on-line* sia già in avanzata fase di realizzazione.

[44] Sono le norme di cui alla nota 41.

[45] Ai sensi delle sezioni 906, 908, 909, 910, E. Giannantonio, *op. cit.*, p. 44.

[46] Così Fabrizio Maimeri, *Contratti bancari*, p. 187, in *Legislazione economica*, dicembre 1982-gennaio 1983, Rassegne e problemi a cura di Francesco Vassalli e Gustavo Visentini, Giuffrè, Milano, 1985.

[47] Così E. Giannantonio, *op. cit.*, pp. 45 e 48 secondo il quale potrebbe anche profilarsi un'illegalità di tale clausola con riferimento all'art. 2698 cod. civ.

[48] Si veda la nota precedente.

preferendo ricercare ed aggregare, in maniera empirica, i casi simili per materia[49].

Nell'EFTA si rinviene la seguente definizione: « il termine "carta accettata o altre forme di accesso" identificano una carta, un codice, o altre forme di accesso al conto di un cliente con lo scopo d'iniziare un trasferimento elettronico di fondi quando la persona per la quale tale carta o gli altri modi di accesso furono emessi ha richiesto e ricevuto o ha firmato o ha usato, o autorizzato un altro ad usare, tale carta o gli altri modi di accesso con lo scopo di trasferire denaro tra conti bancari o prelevare denaro, proprietà, lavoro, o servizi »[50].

Analoga definizione si trova nel *Credit Card Fraud Act of 1984* dove « il termine "strumento di accesso" comprende ogni carta, targhetta, codice, numero di conto, o altri sistemi di accesso al conto che possono essere usati, da soli o insieme ad altri strumenti di accesso, per ottenere denaro, beni, servizi e qualunque altra cosa di valore, o che possono essere usati per iniziare un trasferimento elettronico di fondi (esclusi quelli originati solamente da uno strumento cartaceo) »[51].

Come si potrà notare entrambe le definizioni hanno lo scopo prioritario di comprendere, nella maniera più ampia possibile, l'oggetto tutelato dalla legge per far fronte alle interpretazioni restrittive degli *statutes* da parte delle corti. Entrambe le definizioni, ed è questo il fatto più importante, concepiscono lo « strumento di accesso » — il termine « carta di credito » non viene mai utilizzato — come il mezzo di *accesso al conto per iniziare un trasferimento elettronico di fondi*[52].

Nella dottrina statunitense la carta di credito è stata accostata alla lettera di credito documentaria, in quanto in un rapporto commerciale al debitore si sostituisce un'istituzione meritevole di fiducia (l'istituto finanziario)[53]. La struttura del rapporto è tuttavia diversa ed il raffronto è scarsamente sostenibile. Con la lettera di credito, infatti, in un rapporto commerciale un soggetto vincola l'esecuzione della controparte ad una serie di garanzie da lui predisposte, mentre la carta informatica non ha la funzione di gestione di un contratto, ma quella di permettere al titolare di effettuare una serie di operazioni tra cui quella relativa ai trasferimenti elettronici di fondi.

È stato di recente sostenuto come nelle carte tradizionali la funzione di credito acquisti un ruolo fondamentale anche rispetto al pagamento[54]. Tuttavia nel caso dei trasferimenti elettronici di fondi il pagamento viene adempiuto in tempo reale e quindi, in questo caso, non è possibile sostenere tale interpretazione.

In effetti possiamo definire la carta informatica come uno strumento di legittimazione, cioè il mezzo che tramite un terminale elettronico abilita il titolare, all'immediato, sicuro, personale ed illimitato accesso al proprio conto bancario effettuando una serie di operazioni, tra cui i trasferimenti elettronici di fondi.

In Italia la dottrina oscilla tra chi la definisce come un documento rappresentativo dei fondi esistenti presso la banca e chi la definisce come un documento di legittimazione[55]. In realtà il documento non rappresenta i fondi se non in senso traslato (potendo tali fondi anche mancare); inoltre non sempre la funzione di rappresentatività dei fondi è quella propria della carta potendo l'utente effettuare con la stessa operazioni indipendenti dalla provvista (come versamenti, controlli, ecc.). Ritengo perciò preferibile definire la carta informatica come strumento di legittimazione in quanto essa non può essere intesa, secondo il diritto italiano, come un documento nel senso tradizionale del termine[55-bis].

---

49 M.G. Losano, *op. ult. cit.*, p. 141 e Pietro Rescigno, *Prefazione* a *I trasferimenti elettronici*, cit., p. IX.

50 Definizione in EFTA sec. 903.

51 Sottosezione (e) (1). Per il testo si veda l'Appendice.

52 Si è già sottolineato *supra* (paragrafo 3) la comunanza di questa legge con quella riguardante l'accesso ad un elaboratore.

53 C. Di Nanni, *op. cit.*, p. 57.

54 M. Housemann e H. Berry, *op. cit.*, rispettivamente pp. 75 e 114 e C. Di Nanni, *op. cit.*, *passim*.

55 Nel primo senso P. Nuvolone, *op. cit.*, p. 598; nel secondo Salvatore Maccarone, *op. cit.*, p. 611; G.L. Brancadoro, *op. cit.*, p. 653.

55-*bis* Si veda *infra* il paragrafo 7.

III. L'Analisi del testo del *Credit Card Fraud Act*.

1. Le carenze della legislazione preesistente.

La legislazione penale preesistente alla legge che stiamo esaminando è contenuta in due leggi penali federali del titolo 15 del Codice degli Stati Uniti (U.S.C.). La prima al paragrafo 1644 (*Truth in Lending Act*), rivolta soprattutto alle carte di credito tradizionali, e la seconda al paragrafo 1693n (sezione 916 dell'*Electronic Fund Transfer Act*) rivolta alle carte informatiche.

In realtà i due testi sono esattamente identici, con la sola differenza che la prima usa il termine *credit card* e la seconda *debit instrument*.

Queste leggi prevedevano sette diverse ipotesi di reato, accomunate tra loro dalla necessità che l'illecito riguardasse il commercio federale o con l'estero. Non era invece richiesto in tutti i casi che la condotta illecita fruttasse all'agente un guadagno, nell'arco di un anno, pari o superiore a 500 o 1.000 dollari, a seconda dei casi.

La prima carenza evidenziata dagli operatori del diritto[56] e dalla giurisprudenza era la mancata previsione come reato della contraffazione o alterazione di questi strumenti, fenomeno estremamente generalizzato negli Stati Uniti.

Non era inoltre punito il possesso e l'utilizzazione di attrezzature atte ad alterare o contraffare delle carte.

Altra lacuna riscontrata in quelle leggi era la mancata previsione, come autonoma figura di reato, del possesso di carte (o altri strumenti di pagamento similari) ottenute illecitamente.

In quarto luogo non era certo se queste leggi fossero applicabili al furto, all'uso o alla vendita di ogni strumento o meccanismo che poteva essere usato al posto di un legittimo strumento di pagamento. Problema non irrilevante, che riguardava tutto ciò che non era la carta in sé ma, ad esempio, le copie della ricevuta di vendita o di credito (*sales slips or credit slips*) o il numero di una carta informatica mediante il quale il titolare poteva accedere al proprio conto (PIN). Infatti alcune corti avevano limitato l'interpretazione del termine *card* (ma l'ipotesi era analoga anche per i *debit instrument*) agli atti relativi alle sole carte di credito, e non a quanto relativo alla carta stessa come le *sales slips*, i numeri delle carte di credito e i numeri del PIN. Però questi numeri o le ricevute cartacee potevano essere utilizzati illecitamente con un'altra carta o per forgiare carte in bianco[57].

Un'altra lacuna legislativa riguardava la mancata previsione di un'apposita statuizione che prevedesse come reato l'uso non autorizzato di una carta originariamente ottenuta da un istituto di credito senza intento illecito da parte del titolare della carta stessa e successivamente trasferita ad un'altra persona sapendo che sarebbe stata in seguito illecitamente utilizzata. Ciò, secondo la giurisprudenza, non integrava l'ipotesi di *fraudulently obtained* prevista dalla legge[58].

È inoltre emerso durante gli *hearings* che i malviventi generalmente si tenevano al di sotto della cifra stabilita dalla legge per l'integrazione del reato federale ed utilizzavano diverse carte di debito o di credito, in modo da non incorrere nelle sanzioni previste dalla legge[59].

Le lacune legislative, messe in evidenza dalle corti, avevano definitivamente scoraggiato i Procuratori Federali a far uso delle due leggi sopra indicate, con le quali avevano peraltro scarsa dimestichezza. Poiché non era « inusuale che l'atto criminale violasse anche altri statuti »[60] ritenevano quindi preferibile utilizzare questi ultimi come capo d'accusa principale.

---

[56] J. Keeney, Dip. Giustizia, *Hearings*, p. 154; F. Clarke, FBI, *ivi*, p. 163; Joseph Carlon, Cia, *ivi*, p. 165.

[57] L'interpretazione giurisprudenziale conforme alla lettera degli statuti rinveniva infatti negli stessi la parola, al singolare, *debit instrument*. Così *United States v. Callahan*, 666 F. 2d 422 (9th Cir. 1982). Tuttavia il *Fourth Circuit* in *United States v. Bice-Bey*, 701 F. 2d 1086 (4th Cir. 1983) accolse invece la richiesta del procuratore ritenendo che « l'elemento primario della carta di credito è il suo numero, non il pezzo di plastica ».

[58] Così sentenziato in *United States v. Kasper*, 483 F. Supp. 1208 (D.Pa. 1980).

[59] Così F. Clarke dell'FBI, *Hearings*, secondo il quale nessuna azione penale era stata iniziata fino al 1983 in base all'EFTA 1693n.

[60] Sono quelli riportati da F. Clarke, *Hearings*, cit., nelle note seguenti.

I più frequentemente usati erano il *mail fraud*[61], il *bank fraud and embezzlement*[62], il *bank larceny*[63], l'*interstate transportation of stolen property*[64] e il *wire fraud*[65].

2. I REQUISITI PER INTEGRARE IL REATO FEDERALE.

Per tutte le ipotesi di reato previste, la legge è applicabile « se il reato riguarda il commercio federale o con l'estero » rimandando quindi ad apposite leggi statali la repressione dei reati, di solito di più lieve entità, commessi ed aventi effetti all'interno di un solo stato.

L'esigenza del mantenimento di questa precisa distribuzione di competenze disegnata dalla Costituzione è particolarmente sentita dagli esperti di diritto negli Stati Uniti. Essa garantisce, da un lato, l'autonomia normativa ed istituzionale di ciascuno stato della confederazione rispetto agli organismi federali e, dall'altro, l'operatività di questi ultimi[66].

Nell'usare l'espressione « riguarda il commercio federale o con l'estero » il Congresso ha inteso stabilire un vasto ambito giurisdizionale. L'intenzione era quella di fornire ai Procuratori Federali la possibilità di perseguire effettivamente una grande varietà di frodi realizzate mediante carte di credito e i relativi numeri di conto. Tuttavia, gli importi indicati nella legge — come il valore in dollari per il traffico o l'uso di strumenti non autorizzati — e il possesso di 15 o più strumenti di accesso non autorizzati o contraffatti, assicurano che il coinvolgimento federale si concentri sugli illeciti di maggiore gravità, rispettando la distribuzione di competenze sopra accennata[67].

Si tratta di comportamenti illeciti che devono essere compiuti e dispiegano effetti non nell'ambito di un solo stato, ma rispetto ad una pluralità di stati dell'Unione oppure riguardano il commercio con stati stranieri.

Si noti, in generale, che nell'ambito dei trasferimenti elettronici di fondi gestiti in una rete interbancaria l'agente integra il requisito federale previsto dalle varie figure di reato senza che debba necessariamente superare il confine geografico dello stato o recarsi all'estero. Infatti la frode commessa al terminale della banca di uno stato integra il requi-

---

[61] Il *mail fraud* sanziona l'utilizzazione del servizio postale nella corrispondenza tra diversi stati o con l'estero al fine di progettare od eseguire una frode. L'FBI (si veda la nota precedente) ha rilevato che le frodi relative alle carte di credito in senso lato coinvolgono « generalmente l'uso della posta ». Si pensi ad es. un piano illecito nella realizzazione del quale i malviventi si facciano spedire per posta da una società che le produce ed estranea a tale progetto, carte in bianco oppure si facciano spedire da altri complici carte illecitamente ottenute al fine di falsificarle. Quest'ultima ipotesi potrebbe valere anche nel caso di spedizione postale dei soli numeri delle carte. Questo tipo di frodi sono investigate « in primo luogo » dal *United States Postal Inspection Service* e solo « in un secondo tempo dall'FBI ». Un'interpretazione giurisprudenziale più ampia, tende « a ricondurre nell'ambito del reato di *mail fraud* la responsabilità per violazione dei doveri inerenti i rapporti fiduciari », quando « autore del fatto sia un dipendente o comunque una persona legata al titolare dell'elaboratore da un rapporto fiduciario » G. CORRIAS LUCENTE, *op. cit.*, pp. 184/5 che riporta parte del testo di legge a p. 539). L'Autrice giustamente rileva che « l'orientamento interpretativo invalso per il reato di *Mail Fraud*, incentrando la struttura della fattispecie incriminatrice sulla violazione delle regole comportamentali inerenti i rapporti fiduciari, impedisce di ritenere generalmente sanzionato il furto di servizi dell'elaboratore, in quanto l'uso del *computer*, oltre ad assumere secondario rilievo nell'ambito del fatto punibile, non integra addirittura l'ipotesi di reato in assenza di una relazione a carattere fiduciario fra l'agente ed il titolare dell'elaboratore, o dell'uso del servizio postale ».

[62] Il *bank fraud and embezzlement* sanziona le frodi compiute ai danni di un'istituto di credito quando qualcuno *converts to his own use or the use of another ... money or thing of value of the United States* cioè esercita illecitamente sulla cosa i diritti del proprietario (18 U.S.C. par. 641). Poiché in questi casi oggetto delle frodi è il denaro, non si pongono qui problemi interpretativi, tipici di alcuni reati informatici, riguardo al concetto di « cose di valore ». Per una parziale riproduzione del testo si veda G. CORRIAS LUCENTE, *op. cit.*, p. 185.

[63] Il *bank larceny* è relativo ad alcune fattispecie tipiche del diritto penale statunitense che individuano reati quali il furto e l'appropriazione indebita ma « si diversifica dalle analoghe fattispecie note ai sistemi di *civil law*, innanzitutto in quanto prevede una serie di modalità per la condotta di appropriazione, fra le quali quella di vendere la cosa, ..., in secondo luogo in quanto contempla fra gli oggetti del reato, oltre alle "cose di valore" anche i *records* (cioè qualsiasi informazione trascritta) ». G. CORRIAS LUCENTE, *op. cit.*, p. 523.

[64] L'*interstate transportation of stolen property* sanziona *Whoever transports in interstate or foreign commerce any goods, wares, merchandise, securities, or money of the value of 5.000 dollars or more, knowing the same have been stolen, converted or taken by fraud...* (18 U.S.C. par. 2314).

[65] Il *fraud by wire* sanziona l'utilizzazione di cavi di comunicazione collegati tra diversi stati o con l'estero al fine di progettare od eseguire una frode (18 U.S.C. par. 1342). In tale ambito « sono riconducibili, senza necessità di ricorrere ad artifici interpretativi, anche gli strumenti tecnici che connettono le diverse componenti di un sistema di elaborazione di dati » (G. CORRIAS LUCENTE, *op. cit.*, p. 539).

[66] J. KEENEY, *Hearings*, p. 154 ss.

[67] *Report to accompany H.R. 5616 ABS 1984 H 523-24.*

sito federale se l'istituto di credito ha sede o sportelli in uno stato straniero o in stati diversi da quello dov'è stata effettuata la frode. Viceversa non vi sarà reato federale nel caso di un istituto di credito che abbia la propria sede e i propri terminali distribuiti all'interno di un solo stato.

La condotta illecita costituisce inoltre reato federale qualora si sia realizzata anche al di là del confine geografico di un singolo stato (cioè in più stati o in uno stato nazionale ed estero). Anche in questo caso occorre però che soggetto passivo dell'illecito non sia un istituto di credito operante solo nell'ambito di uno stato.

Passando brevemente in rassegna le varie figure di reato rileviamo quindi che la produzione di strumenti contraffatti, l'uso o il traffico di uno o più strumenti di accesso contraffatti o non autorizzati (indipendentemente dal fatto che la condotta si sia svolta in uno o più stati o all'estero) deve essere relativa a carte circolanti in più stati o all'estero. Lo stesso dicasi per il possesso di almeno 15 strumenti di accesso contraffatti o la produzione, traffico, controllo, custodia o possesso di attrezzature per realizzare strumenti di accesso.

3. Gli altri requisiti.

La legge è stata collocata dal legislatore, nell'ambito del diritto penale statunitense, nel capitolo relativo alle frodi e alle false attestazioni[68] e tale scelta è giustificata sia dalle fattispecie previste sia dalla dizione letterale del testo (*Fraud and related activity...*).

Le singole fattispecie non riguardano però solo reati di frode[69] ma anche quello di contraffazione (*counterfeiting* comprendente anche il reato di falsificazione o *forgery*)[70] e la previsione di uno specifico ed autonomo reato possessorio[71].

Si può subito rilevare da un punto di vista generale come, a differenza di alcuni sistemi di *civil law*, il legislatore americano sia più elastico nell'individuazione degli elementi necessari ad integrare una frode, prevedendo di volta in volta a seconda della necessità, autonome figure di reato che « prescindono sia dall'acquisito vantaggio patrimoniale in capo all'agente, sia dal pregiudizio economico della parte offesa, sia dall'induzione in inganno di una persona »[72]. Fa eccezione a quanto sopra solo l'ipotesi di cui al punto (a) (2) in cui il soggetto deve ottenere un illecito vantaggio patrimoniale pari o superiore a 1.000 dollari durante il corso di un anno.

Un altro requisito, oltre a quello federale, è richiesto dalla legge in ciascuna fattispecie. Si tratta della particolare qualificazione dell'elemento psicologico o *mens rea* che prevede tanto la « conoscenza » che « l'intento di frodare »[73].

La dottrina statunitense distingue due tipi di « intento » illecito: uno generico e l'altro specifico[74].

L'*intent* specifico è l'atteggiamento mentale che rappresenta la volontà del soggetto agente di causare un evento dannoso proibito dalla legge[75]. Richiede quindi un determinato grado di certezza per quanto riguarda la condotta adottata e di consapevolezza per i risultati previsti. La certezza è assicurata dalla conoscenza[76] cioè dalla percezione sicura

---

[68] *Chapter 47 - Fraud and false statements.*

[69] Ipotesi *sub* (a) (1) e (a) (2) e per le quali si veda il testo di legge in appendice.

[70] Ipotesi *sub* (a) (1) e (a) (4).

[71] Ipotesi *sub* (a) (3).

[72] G. Corrias Lucente, *op. cit.*, p. 539 con riguardo ai reati di *wire* e *mail fraud*.

[73] L'elemento soggettivo o *mens rea* viene interpretato in modi diversi nel diritto americano. Le due teorie dominanti si rifanno ad una concezione oggettiva ed una soggettiva. Per una rassegna di tali concetti si veda Cherif M. Bassiouni, *op. cit.*, p. 207 ss.

[74] La distinzione tra dolo e colpa non è stata fatta propria dagli ordinamenti giuridici penali di *common law*. Tuttavia questa diversificazione riappare nella distinzione che viene operata tra *intent* generico e specifico ed in definitiva il risultato ultimo dei due sistemi è molto simile. Si veda C. Bassiouni, *op. cit.*, p. 215 ss. Ci si riferisce all'*intent* specifico in termini d'intenzione e conoscenza mentre l'*intent* generico riguarda la prevedibilità (*foreseeability*) *la noncuranza* (*recklesness*) *e la negligenza criminosa* (*criminal negligence*). Tutte le forme d'*intent* fanno parte dell'elemento soggettivo ed ogni singolo reato può richiedere una o più di queste forme d'*intent*.

[75] Il termine « con l'intento » è stato usato dal Congresso per indicare il colpevole stato mentale che ha il termine proposito (*purpose*) usato nel nuovo progetto di *Model Penal Code* (# 2.02).

[76] La conoscenza fa quindi parte dell'*intent specifico*. Per questo concetto si veda C. Bassiouni, *op. cit.*, p. 220 ss. « La distinzione dallo stato mentale di conoscenza era stata recentemente ristabilita dal giudice Rehnquist, Come abbiamo messo in luce nella sentenza *United States v. United States Gypsum Co.*, 438 U.S. 422, 445 (1978), una persona che causa un particolare risultato si dice che agisca di proposito se « egli coscientemente desideri quel risultato, qualunque sia la probabilità di quel risultato derivante dalla sua condotta », mentre si dice che agisca con conoscenza se egli è conscio « che questo risultato è praticamente

che quel dato fatto, in conseguenza delle leggi scientifiche o naturali, produrrà quel determinato risultato. Dai lavori preparatori alla legge possiamo rilevare che uno stato mentale di conoscenza rispetto ad un elemento del reato è 1) la coscienza della natura della propria condotta, e 2) la coscienza di o una ferma certezza dell'esistenza di una circostanza rilevante (ad esempio, che uno strumento di accesso era contraffatto prima di essere usato o trasferito ad altri). Il Congresso ha ritenuto che « il requisito dello stato mentale di conoscenza possa essere soddisfatto dalla prova che l'attore era cosciente dell'alta probabilità di esistenza di tale circostanza, sebbene la difesa possa avere successo qualora riesca a provare che l'imputato credeva, in quel momento, dopo aver intrapreso le ragionevoli azioni per garantire tale convinzione, che tale circostanza non esistesse ».

La condotta illecita dell'agente integra il reato anche se è conosciuta dal terzo coinvolto (per esempio, il commerciante che è perfettamente conscio del fatto che il compratore usi carte contraffatte, e perciò non è vittima della frode).

Occorre inoltre ricordare che, nell'ipotesi *sub* (a) (4), l'intento di frodare non è solo quello che il soggetto usi egli stesso l'apparecchiatura per compiere la frode, quanto piuttosto che quell'attrezzatura sarà usata da lui o da un altro per commettere frodi. Ciò è di grande importanza, in quanto qualifica come illecita un'attività che potrebbe essere altrimenti considerata lecita (come un deposito per conto terzi o la costruzione di macchine per fare carte di credito). Il depositario o i responsabili della ditta specializzata nella produzione di quelle apparecchiature per conto terzi qualora sappiano dell'intento illecito dei malviventi, subiranno le pene previste dalla legge[77].

Assume particolare importanza, nel caso di *intent specifico*, il regime della prova in generale[78] e l'onere probatorio posto a carico delle parti. Nei reati ad intenzione generica l'intenzione criminosa richiesta viene presunta dal fatto stesso della commissione del reato. Nei processi in cui si richiede un *intent* generico, una volta dimostrata la commissione del reato, la sua mancanza può essere eccepita dall'accusato, ma l'onere della prova è a suo carico. Invece nei reati in cui si richiede un *intent* specifico, la sua esistenza deve essere dimostrata dallo Stato[79].

Nel reato possessorio *sub* (a) (3) l'*intent* si basa sul presupposto che il fatto stesso del possesso (in certi reati in cui è fatto divieto ad una persona di detenere un determinato oggetto), è sufficiente a creare una presunzione relativa di comportamento intenzionale. Quindi, in tali reati, l'elemento mentale (soggettivo) dell'*intent* o della conoscenza si presume dal fatto stesso del possesso e non è necessario che l'accusa ne dia prova; però la difesa può eccepirne l'assenza[80].

L'elemento oggettivo o *actus reus*[81] previsto dalla legge consiste in quattro diverse condotte[82], nel tentativo e nel concorso.

Le fattispecie sono caratterizzate da condotte positive o negative sufficientemente chiare per non ripeterle ulteriormente e quindi qui basterà dare solo qualche spiegazione dei punti più interessanti.

L'ipotesi *sub* (a) (1) non stabilisce alcun limite in denaro per far considera-

---

certo derivare dalla sua condotta, qualunque possa essere il suo desiderio rispetto a quella condotta. *United States v. Bailey*, 444 U.S. 394, 404 (1980) » *Report*, cit., p. 16.

77 In tal senso il *Report*, cit., p. 16 ss.

78 « Ogni forma di *intent* che è richiesta per un determinato reato deve essere dimostrata al di là di ogni ragionevole dubbio, come ogni altro elemento del reato. Ciò che differenzia queste diverse forme d'*intent* non è il *quantum* della prova richiesta, che non deve mai lasciare adito a dubbi, ma ciò che deve essere provato. I reati ad *intent* specifico richiedono la dimostrazione certa o quasi certa dell'*intent* di una persona di fare qualcosa e di produrre un dato risultato, mentre l'*intent* generico richiede la dimostrazione della prevedibilità basata su una data deviazione da criteri di condotta riferiti alla persona di comune diligenza ». C. BASSIOUNI, *op. cit.*, p. 219.

79 *State v. Jamison*, 517, P. 2d 1241, 110 Ariz. 245, 1974. In questo caso si doveva in particolare esaminare il rapporto tra *intent* ed intossicazione volontaria. La corte ha stabilito che tale intossicazione non fa venire meno l'*intent* generico mentre può costituire causa di esclusione o diminuzione di responsabilità dell'*intent* specifico.

80 C. BASSIOUNI, *op. cit.*, p. 229.

81 La definizione del concetto e delle caratteristiche dell'elemento oggettivo o *actus reus* (« ogni atto o serie di atti volontari, o condotta che determini certe circostanze materiali o fisiche, sia in modo diretto che indiretto, attraverso l'intervento o la mediazione di altri » CLARK e MARSHALL, *Crimes*, ed Wingersky, 1958, p. 176) assume, com'è noto, primaria importanza nel diritto penale.

82 Al termine atto viene preferito quello di condotta in quanto più vasto e comprendente le manifestazioni materiali, sia attive che passive, compiute volontariamente da un soggetto. Così C. BASSIOUNI, *op. cit.*, p. 198.

re questa condotta come reato federale. Si tratta infatti di comportamenti considerati già di per sé estremamente gravi, in quanto relativi a strumenti di accesso contraffatti. La Camera dei Rappresentanti ha infatti ritenuto che « la contraffazione di tali carte è analoga alla contraffazione della valuta degli U.S.A. »[83]. Si noti ancora l'importanza della previsione legislativa secondo la quale la condotta può riguardare uno o più strumenti di accesso[84].

La seconda (a) (2), consistendo in comportamenti relativi a strumenti di accesso non autorizzati, è stata considerata meno grave della precedente ed è stato quindi fissato un importo massimo d'illecito guadagno pari a mille dollari durante qualsiasi periodo di un anno. Questo limite si adegua ai livelli stabiliti per i reati sanzionati nel *Truth in Lending Act* e nell'*Electronic Funds Transfer Act*. Anche in questo caso il legislatore ha avuto cura di specificare che la condotta può riguardare uno o più strumenti di accesso per ottenere quella cifra.

La terza (a) (3) prevede un reato possessorio integrato dal possesso di almeno 15 strumenti di accesso contraffatti o non autorizzati e prescinde da qualsiasi condotta illecita precedente. Il proposito della limitazione numerica è quello di concentrare gli sforzi del Governo Federale sui maggiori trafficanti e contraffattori e di autorizzarne il coinvolgimento anche nei casi in cui la produzione, il commercio o l'uso di questi strumenti di accesso non possa essere stabilito. Qualunque combinazione di strumenti di accesso contraffatti o non autorizzati è sufficiente per integrare la fattispecie[85].

La quarta (a) (4) consiste nella produzione, traffico, controllo, custodia o possesso di attrezzature per produrre strumenti di accesso. Il reato è sufficientemente grave da garantire l'inizio dell'azione penale senza alcun limite d'importo. Il malvivente non deve necessariamente avere il possesso fisico dell'attrezzatura, purché egli abbia il controllo sull'attrezzatura che sia nel possesso di un altro. La condotta illecita, accompagnata dall'*intent* di frodare nel senso sopra esaminato, potrà perciò essere realizzata da lui stesso o da un altro per commettere la frode[86].

La quinta (b) (1) riguarda il tentativo di commettere un reato previsto nelle precedenti quattro ipotesi. È un'autonoma ipotesi di reato in cui acquista particolare rilievo il rapporto tra fase ideativa (di per sé non punibile) e fase esecutiva del piano criminoso. Sarà poi un problema di fatto stabilire quando le azioni del soggetto cominciano ad estrinsecarsi in una condotta oggettivamente criminosa ai sensi di una determinata legge.

La sesta ed ultima ipotesi (b) (2) prevede il concorso di due o più persone ad un progetto per commettere un reato previsto nelle precedenti ipotesi *sub* (a). Affinché ricorra questo reato associativo occorre che 1) il progetto criminoso riguardi uno dei reati previsti da questa legge nella sottosezione (a); 2) vi sia il concorso di due o più persone in quel progetto 3) una qualunque delle parti si sia impegnata in qualsiasi comportamento per la realizzazione del reato. È una previsione sufficientemente ampia per comprendervi tutti quei comportamenti non implicanti un coinvolgimento diretto nell'azione da parte di persone che si limitano ad un supporto tecnico o d'informazione. Vengono così scoraggiate le collusioni tra malavita organizzata e *colletti bianchi* allettati dal raggiungimento di facili ed immediati guadagni. Tuttavia il concorso in un reato non giustifica una sanzione pari o superiore a quella del reato consumato o tentato e, per questa ragione, la pena comminata dalla legge in questo caso è più lieve.

Inoltre, secondo i principi generali del diritto penale statunitense, per integrare l'ipotesi di reato occorre che ci sia il concorso degli elementi oggettivi e soggettivi[87] ed il nesso di causalità tra la condot-

---

[83] *Report*, cit., p. 17.

[84] Per tale importanza si veda *supra* il paragrafo 1 e la nota n. 59.

[85] Si veda la nota n. 83.

[86] *Report*, cit., p. 18.

[87] « Né l'*intent* da solo, né la condotta da sola sono sufficienti a soddisfare i requisiti del reato. Occorre che entrambi gli elementi siano presenti e concorrenti. La necessità del concorso degli elementi del reato nasce dal fatto che l'*intent* criminoso si manifesta nella condotta del soggetto agente e tale condotta riflette l'intento criminoso se si vuole distinguere un reato da un semplice accadimento o da un evento fortuito. Una persona può inavvertitamente cagionare un danno e poi, magari, rallegrarsene, ma questo non è « reato ». C. BASSIOUNI, *op. cit.*, p. 238 ss. Si veda ad esempio *Jackson v. Commonwealth*, 100, Ky. 239, 38 S.W. 422, 1968, in cui si l'agente ritenendo di aver ucciso la vittima, che era però sopravvissuta, la uccise effettivamente in un secondo tempo.

ta dell'agente e l'evento dannoso penalmente sanzionato[88].

4. La terminologia usata.

Occorre a questo punto sottolineare come il legislatore statunitense si sia preoccupato, secondo una prassi ormai in uso da tempo, di prevedere nella stesura del testo un'apposita sezione dedicata specificamente alla definizione della terminologia usata[89]. Inoltre si è preoccupato di usare un linguaggio di facile lettura e comprensione anche per i non addetti ai lavori, senza per questo tralasciare il necessario tecnicismo[90].

La definizione di *strumento di accesso*[91] è stata formulata in modo da ricomprendervi i futuri cambiamenti tecnologici. La sola limitazione posta (« esclusi quelli originati solamente da uno strumento cartaceo ») esclude attività quali quelle relative ad assegni falsi.

La frase *da solo o insieme ad altri strumenti di accesso* comprende qualunque mezzo di accesso al conto o termine d'identificazione della carta informatica attualmente in uso o che potrebbe diventare tecnologicamente possibile, che può essere usato in connessione con delle carte ma che, da solo, non è uno « strumento di accesso ». Un esempio di questo sarebbe il numero d'identificazione personale (PIN) che può essere usato in connessione con strumenti di accesso[92].

Uno *strumento di accesso contraffatto* è[93] qualunque strumento di accesso che sia contraffatto, fittizio, alterato o falsificato o un componente identificabile di uno strumento di accesso o di uno strumento di accesso contraffatto.

Il termine *fittizio* si riferisce a diversi tipi di strumenti contraffatti, incluse le riproduzioni, i dipinti o facsimile di uno strumento di accesso. La definizione vuole essere sufficientemente ampia da comprendere componenti di uno strumento di accesso o di uno strumento di accesso contraffatto, ma esclude le materie prime non distinguibili. Cadrebbe così nella definizione di strumento di accesso contraffatto ogni componente identificabile ottenuto in qualche modo da un malvivente con l'intento di frodare o un falso o contraffatto sostituto di un originale componente.

Il termine *componente* include gli strumenti di accesso o gli strumenti di accesso contraffatti incompleti, così come strisce magnetiche, ologrammi, firme, pannelli, microchips, e le carte di credito in bianco (le così dette *white plastic*).

Per *strumenti di accesso non autorizzati*[94] s'intende ogni strumento che è perso, rubato, scaduto, revocato, cancellato od ottenuto con l'intento di frodare. Il Congresso ha così operato una netta distinzione tra « strumenti di accesso contraffatti » e « non autorizzati ». I primi implicano un'attività illecita — a livello individuale o collettivo — di contraffazione o falsificazione di un valido strumento di accesso per il suo utilizzo ai fini di frode. La seconda riguarda l'utilizzo di una carta scaduta o revocata o cancellata da parte del legittimo proprietario che consapevolmente ne faccia un uso illecito, o l'utilizzo illecito di una carta non autorizzata da parte di terzi. Quest'ultima attività non implica la con-

---

88 Il comportamento del reo deve riflettere la sua intenzione e deve costituire la causa diretta, immediata e determinante dell'evento. In questo senso un soggetto non può essere responsabile delle 1) conseguenze remote ed indirette che secondo il normale buon senso non si poteva prevedere che scaturissero da tale comportamento o 2) di quelle conseguenze che si sarebbero potute verificare a prescindere dal comportamento dell'agente. Ogni causa indipendente che sia intervenuta, interrompe il nesso causale tra il comportamento iniziale dell'agente e l'offesa od il danno subiti dalla vittima. Invece, una causa sopravvenuta dipendente dalla condotta dell'agente non interrompe il nesso causale poiché si tratta di un fattore prevedibile (se non addirittura mediato dell'agente) alla luce dell'interazione tra il comportamento dell'agente ed altri eventi e circostanze di normale previsione. L'agente non è tenuto a prevedere l'evento specifico, ma soltanto il tipo di evento che è probabile e ragionevole attendersi. Considerazioni tratte da C. Bassiouni, *op. cit.*, p. 240. Si veda inoltre *State v. Glover*, 330 Mo. 709, 50 S.W. 2d 1049, 1932 nel quale la Corte ha pronunciato una sentenza di omicidio di primo grado contro una persona che aveva « intenzionalmente » dato fuoco ad un drugstore provocando la morte di un vigile del fuoco accorso per spegnere le fiamme.

89 Tale sezione rappresenta circa un quarto dell'intero testo.

90 È stato scritto che uno dei primi requisiti di un'informazione giuridica democratica riguardo alla legislazione si basa su una « redazione sintatticamente piana, logicamente e terminologicamente rigorosa ma per quanto possibile vicina al linguaggio comune, per quanto possibile concreta... ». Luigi Lombardi Vallauri, *Democraticità dell'informazione giuridica ed informatica*, in *Informatica e diritto*, Le Monnier, Firenze, 1975, p. 4. C'è motivo di riflessione anche per il nostro legislatore.

91 Sottosezione (e) (1).

92 Per questa e le ulteriori indicazioni contenute in questo paragrafo riguardanti le definizioni si veda il *Report*, cit., p. 19.

93 Sottosezione (e) (2).

94 Sottosezione (e) (3).

traffazione o falsificazione della carta e pertanto qualora l'illecito guadagno non superi i mille dollari durante un anno è considerata di minore gravità e si è ritenuto che sia più appropriamente perseguita dallo Stato e dalle autorità locali o in azioni civili da parte degli istituti emittenti.

Il termine *produce*[95] è inclusivo di disegnare, alterare, autenticare, duplicare, o assembleare ed è usato in connessione con strumenti di accesso contraffatti o con apparecchiature per la loro costruzione.

Il termine *traffica*[96] comprende l'azione di chi trasferisce o altrimenti dispone di, verso un altro, o ne detiene il controllo, con l'intento di trasferire, di disporre, di contraffare sia strumenti di accesso non autorizzati che attrezzature per la produzione di strumenti di accesso. In questo termine sono inclusi i concetti di comprare, vendere, trasferire, ricevere, prestare, distribuire, affittare o dare in proprietà.

Attrezzatura per realizzare strumenti di accesso[97] comprende, ad esempio, un equipaggiamento destinato ad un vasto campo di attività, una delle quali è collegata all'illegale produzione di strumenti di accesso. Non si è inteso cioè limitare l'ambito della parola *progettato* ai soli equipaggiamenti costruiti appositamente per fare carte di credito. I macchinari aventi quindi la possibilità di costruire carte di credito informatiche ed altri tipi di carte (per es. carte magnetiche per l'uso del telefono o per l'accesso ad un ufficio) rientrano in questa previsione.

5. Il regime delle sanzioni.

Le pene previste nella sottosezione (c) della legge per il reato consumato, il tentativo ed il concorso nello stesso sono graduate, conformemente al *False Identification Crime Control Act of 1982* (18 U.S.C. 1028), in relazione alla gravità dei reati, ai danni risultanti ed alla recidiva.

Le sanzioni previste nella sottosezione (c) (1) prevedono una pena pecuniaria non superiore all'importo di $ 10.000 o il doppio del valore ottenuto dal reato[98], oppure una pena detentiva non superiore a 10 anni, o entrambe.

Inoltre le pene aumentano considerevolmente nella sottosezione (c) (2) che prevede una pena pecuniaria non superiore all'importo di $ 50.000 o il doppio del valore ottenuto dal reato, oppure una pena detentiva non superiore a 15 anni, o entrambe[99].

L'ultima sottosezione (c) (3) considera appositamente i casi di recidiva alle ipotesi precedenti per comminare il massimo delle sanzioni: pena pecuniaria non superiore all'importo di $ 100.000 o il doppio del valore ottenuto dal reato oppure una pena detentiva non superiore a 20 anni, o entrambe.

Il tentativo di reato è equiparato, dal punto di vista sanzionatorio, al reato consumato[100] e quindi si applicano le pene relative alla fattispecie che l'imputato ha cercato di realizzare[101]. Si noti che in questo caso, poiché il reato non è stato consumato, non è possibile ipotizzare come alternativa alla pena pecuniaria il doppio del valore ottenuto dal reato.

Oltre al reato consumato e tentato è punito anche il concorso nel reato. In quest'ultimo caso le pene pecuniarie rimangono invariate rispetto ai casi di reato consumato mentre la sanzione detentiva potrà al massimo raggiungere la metà di quella prevista per il reato consumato[102]. Occorre ancora rilevare che il legislatore, in questo caso, non ha voluto prendere in considerazione l'ipotesi della recidiva. Infatti la legge prende esplicitamente in esame solo la recidiva per il reato consumato o per il « tentativo di commettere un reato », escludendo così esplicitamente l'applicabilità delle sanzioni relative alla recidiva nell'ipotesi del concorso[103].

---

95 Sottosezione (e) (4).

96 Sottosezione (e) (5).

97 Sottosezione (e) (6).

98 Relative ai casi *sub* (a) (2) e (a) (3) e, si noti bene, *in assenza di recidiva*. Qualora infatti ricorra la recidiva si dovrà utilizzare la sottosezione (c) (3).

99 Relative ai casi *sub* (a) (1) e (a) (4) ed anche in questo caso in assenza di recidiva (si veda la nota precedente).

100 Si veda il punto (b) (1) della legge in appendice. Si tratta di una previsione abbastanza severa che cerca così di scoraggiare tutti quei « colletti bianchi » che volessero intraprendere o continuare la carriera criminosa in questo delicato settore.

101 Così ad es. se il tentato reato è relativo alla fattispecie di cui al punto (a) (1), in assenza di recidiva le sanzioni applicabili saranno quelle previste alla sottosezione (c) (2), altrimenti si applicheranno quelle della sottosezione (c) (3).

102 Se, per es., il concorso riguarda la produzione di strumenti di accesso contraffatti, ipotesi *sub* (a) (1) la pena sarà fino ad un massimo di $ 50.000 o sette anni e mezzo di detenzione o entrambe.

103 Si veda il combinato disposto della sottosezione (b) (2) e (c) che escludono l'applicabilità del punto (c) (3).

Il regime sanzionatorio così delineato prevede solamente reati gravi o *felonies*[104] e costituisce un considerevole inasprimento delle pene previste nel *Truth in Lending Act* e nell'*Electronic Fund Transfer Act*[105].

Si tratta inoltre di sanzioni molto elastiche che consentono « al giudice un elevato margine di discrezionalità in ordine alla concreta inflizione della pena — riconoscibile nella possibilità di applicare anche la sola pena pecuniaria e nell'omessa determinazione del minimo edittale »[106].

Quest'ampia discrezionalità è dovuta al fatto che l'informatica può costituire il mezzo per la realizzazione di un grande numero di illeciti estremamente diversificati sia per il tipo di reato compiuto, sia per il soggetto che li pone in essere. In questo senso le diverse motivazioni (*motive*) della condotta possono anch'esse incidere nella valutazione della sanzione. Si pensi, nell'ambito delle carte informatiche, alla differenza tra la frode compiuta dal titolare della carta (con uno strumento non autorizzato), da un'organizzazione criminale (con strumenti contraffatti) o da un giovane *hacker*. In quest'ultimo caso le motivazioni ludiche (che si concretano nel prelievo di un dollaro), luddistiche (devastazione archivi informatici e prelievo di un dollaro) o fraudolente (prelievo di 100.000 dollari) possono influire sulla concreta irrogazione della pena[107]. Per questa ragione la dottrina statunitense, accanto alle sanzioni penali, i cui innegabili effetti deterrenti e repressivi sono tenuti in grande considerazione, dà una certa importanza anche alle sanzioni civili[108].

6. Investigazioni e verifica dell'efficacia.

La complessità dell'ordinamento statunitense ha sollecitato il legislatore ad inserire un'apposita statuizione che prevedesse l'investigazione di questi reati da parte del Servizio Segreto[109], in aggiunta ad ogni altro organismo ed in accordo con il *General Attorney*[110]. L'intento d'impedire che altre agenzie federali a ciò preposte per legge rimanessero escluse dal compimento delle loro indagini ha ispirato la sottosezione (f).

I procedimenti penali relativi a questa legge sono stati 104 nel 1985 e 616 nel 1986, come risulta dalle relazioni presentate al Congresso dal *General Attorney* in ottemperanza alle disposizioni della sezione 1603[111].

Il favorevole accoglimento di questa legge da parte dei Procuratori Federali e l'effetto deterrente della stessa pare abbiano contribuito in maniera determinante a diminuire le frodi compiute nel 1985/6 ai danni degli istituti di credito[112].

Tuttavia le frodi relative alle carte informatiche costituiranno sempre, nonostante i progressi tecnologici compiuti, un problema della nostra società, trattandosi di attività illecite altamente remunerative e di difficile investigazione.

---

104 La distinzione tra reati gravi detti appunto *felonies* e reati meno gravi o *misdemeanors* corrisponde grosso modo alla distinzione che esiste nel nostro ordinamento tra delitto e contravvenzione (in questo senso C. Bassiouni, *op. cit.*, pp. 100 e 113) e comporta differenze in ordine alla disciplina dell'arresto, a quella della fase istruttoria e dibattimentale e, in caso di condanna, sul luogo di detenzione. I primi sono reati che prevedono una pena detentiva superiore ad un anno i secondi la reclusione non superiore ad un anno o una pena pecuniaria (Vittorio Fanchiotti, *op. cit.*, p. 57).

105 Dove le pene erano semplicemente « una pena pecuniaria non superiore a 10.000 dollari o detentiva non superiore a 10 anni o entrambe ».

106 G. Corrias Lucente, *op. cit.*, p. 551.

107 Il superamento delle protezioni degli elaboratori da parte degli *hackers*, anche nei casi meno pericolosi, è estremamente temibile e provoca notevoli danni economici indipendentemente dal compimento di altri reati. Anche quando non sono stati danneggiati gli archivi informatici occorre ricontrollarli ed apprestare nuove difese logiche per impedire ulteriori intrusioni.

108 In questo senso Colin Tapper, *Computer Law*, Longman, London New York, 3th ed. 1983, p. 97.

109 Si veda la sottosezione (d). Il Servizio Segreto dipende gerarchicamente dal Dipartimento del Tesoro.

110 Il *General Attorney* corrisponde, grosso modo, al nostro Ministro della Giustizia e da lui dipendono gli uffici dell'FBI. L'accordo in questione è stato raggiunto nell'agosto del 1985 ed attribuisce alla Cia la responsabilità delle investigazioni relative alle frodi compiute al di fuori degli istituti di credito ed all'FBI quelle compiute all'interno di tali istituti.

111 Le frodi compiute nel 1985 e 1986 erano così suddivise per sottosezione: (a) (2) 39 e 49%; (a) (1) 20 e 13%; (a) (3) 17 e 13%; (b) (1) 12 e 6,5%; (b) (2) 9 e 15%; (a) (4) 3 e 3,5%.

112 Si veda la relazione presentata dal *General Attorney* al Congresso nel 1986 dove la *Visa* dichiara che le perdite dovute a contraffazione « si sono ridotte a livelli veramente bassi » raggiungendo « nell'ambito Visa minimi storici in relazione alle percentuali di vendita ». Più articolato è il giudizio dell'*American Express* che ritiene la legge « un importante passo perché siano destinate al successo le iniziative penali a livello federale contro i nuovi e sempre diversi tipi di crimini finanziari » e dà un giudizio positivo sull'accordo e sulle investigazioni compiute da FBI e Servizio Segreto.

7. CENNI DI DIRITTO PENALE ITALIANO.

Non esiste in Italia, al pari degli U.S.A., una norma che sanzioni gli illeciti compiuti mediante carte informatiche Bancomat.

Occorre quindi esaminare l'applicabilità di alcune norme del codice penale che si potrebbero prestare alla repressione di questi illeciti.

Anche per le carte Bancomat si può ipotizzare sia la loro falsificazione, sia l'illecita sottrazione al legittimo proprietario.

La prima ipotesi viene ritenuta non punibile da parte della dottrina che, con argomentazioni peraltro convincenti, ritiene non assimilabili i documenti tradizionali e quelli di origine informatica. In essi mancherebbe infatti l'incorporazione in un supporto cartaceo, la funzione di comunicazione e la riconoscibilità della provenienza da un soggetto determinato. Sembra infatti che riguardo a questi punti le tessere Bancomat, pur con qualche dubbio, non possano essere assimilate ad un documento. Mancano, infatti, sia la caratteristica incorporazione in un supporto cartaceo sia la funzione di comunicazione tra due soggetti proprie dei documenti. La riconoscibilità della provenienza da un soggetto determinato può invece essere soddisfatta dall'indicazione, posta sulla tessera, delle generalità del titolare della stessa. In base a queste considerazioni viene quindi a mancare il tipico oggetto del falso[113].

Nella seconda ipotesi, si potrebbe profilare un autonomo reato di furto, nel caso d'illecita sottrazione; ovvero un'aggravante del furto principale, nel caso vengano successivamente usate le carte rubate[114].

La qualificazione della condotta relativa all'illecito utilizzo di una tessera contraffatta o non autorizzata va poi distinta a seconda dell'operazione che il soggetto intende compiere. Si tratta di una distinzione importante perché essa avrà effetti giuridici diversi a seconda che venga effettuato un trasferimento elettronico di fondi o un prelievo di denaro.

Nel primo caso la tessera può essere utilizzata in modo illecito in un Punto di Vendita. Tuttavia, in assenza di un'apposita regolamentazione contrattuale di queste operazioni, non è possibile sapere *a priori* se il danneggiato è la banca o il commerciante. Non è quindi possibile qualificare penalmente questa condotta poiché non è individuato il danneggiato[115]. Si può comunque rilevare che in questo caso è difficile ipotizzare il reato di furto o di appropriazione indebita, mentre pare più ragionevole inquadrare la fattispecie nel reato di truffa. In effetti qui si verifica un'attività dell'agente volta a danneggiare mediante artifici il terzo e non la semplice apprensione materiale della cosa (requisito indispensabile per l'integrazione del furto)[116].

Come si può qualificare invece la condotta nel secondo caso e cioè quando il soggetto compia un'operazione di prelievo? Occorre qui distinguere due ipotesi. La prima è relativa all'abuso del servizio Bancomat da parte del correntista. Qualcuno ha rilevato un'analogia con il reato di emissione di assegni a vuoto; altri ritengono che si tratti di concessione di un fido anomalo; altri — secondo un'argomentazione che mi pare più convincente — che tale comportamento integri il reato di furto[117]. La seconda ipotesi riguarda l'illecito utilizzo della tessera da parte di persona non titolare della stessa. È stato profilato il reato di truffa sia nel caso di sottrazione della carta al legittimo proprietario, sia nel caso di falsificazione della stessa, sia nel caso di conoscenza casuale o illecita del PIN[118]. Si tratterebbe di una truffa ai danni del legittimo titolare con induzione in errore della banca. Tuttavia mi sembrano più appropriate le considerazioni sostenute da altra dottrina, secondo la quale non sarebbe integrato il reato di truffa sia perché l'induzione in

---

113 Così L. PICOTTI, *op. cit.*, pp. 952 e 958 ss. che esclude anche l'applicabilità alle tessere Bancomat dell'art. 458 cod. pen. relativo alle carte di credito pubbliche ed equiparate; e inoltre G. CORRIAS LUCENTE, *op. cit.*, p. 535. *Contra*: P. NUVOLONE, *op. cit.*, che ritiene applicabile il reato di falso in scrittura privata.

114 Così L. TRIA, *op. cit.*, p. 294 e P. NUVOLONE, *op. cit.*, per la prima ipotesi.

115 G. CORRIAS LUCENTE, *op. cit.*, p. 544.

116 L. PICOTTI, *op. cit.*, p. 951 e G. CORRIAS LUCENTE, *op. cit.*, p. 545; *contra*: L. TRIA, *op. cit.*, p. 294.

117 Per la prima ipotesi P. NUVOLONE, *op. cit.*, p. 599; L. TRIA, *op. cit.*, p. 292 e E. GIANNANTONIO, *op. cit.*, p. 50 che però non prende posizione; per la seconda F. MAIMERI, *op. cit.*, p. 179; per l'ultima G. CORRIAS LUCENTE, *Bancomat e rilevanza penale dell'abuso da parte del correntista*, *DII*, 1985, p. 726 ss.

118 P. NUVOLONE, *op. cit.*, p. 599.

errore deve essere riferita ad una persona fisica, sia perché non è possibile considerare tale l'elaboratore[119]. In questo caso, la particolarità dell'operazione, nella quale avviene l'erogazione materiale delle banconote da parte della macchina, consente d'inquadrare l'ipotesi nel reato di furto.

È tuttavia opportuno un intervento del legislatore per regolare civilmente e penalmente questa complessa materia[120].

FRANCESCO MANINI

[119] A. TRAVERSI, *op. cit.*, p. 192; L. PICOTTI, *op. cit.*, p. 951; G. CORRIAS LUCENTE, *Informatica e diritto penale*, cit., p. 542 e ID., *Bancomat e rilevanza penale*, cit., p. 726.

[120] Anche il legislatore francese ha recentemente provveduto, con la legge n. 88-19 del 5 gennaio 1988, ad aggiungere al codice penale un apposito capitolo relativo alle frodi informatiche. Il testo è riportato in questa *Rivista* 1988, 645.

APPENDICE

LEGGE PUBBLICA 98-473 DEL 12 OTTOBRE 1984 - 98 *STATUTES AT LARGE* 2183 CAPITOLO XVI - FRODE CON CARTA DI CREDITO.

Sezione 1601. — Questo capitolo può essere citato come il « *Credit Card Fraud Act* del 1984 ».

Sezione 1602.

(a) Il capitolo 47 del titolo 18 del Codice degli Stati Uniti è modificato mediante l'aggiunta alla fine dello stesso di quanto segue:

« # 1029. — Frode e attività connesse in relazione ai sistemi di accesso.

(a) Chiunque —

(1) con conoscenza e con l'intento di frodare produca, usi o traffichi con uno o più strumenti di accesso contraffatti;

(2) con conoscenza e con l'intento di frodare traffichi con o usi uno o più strumenti di accesso non autorizzati durante qualunque periodo di un anno, e mediante tale condotta ottenga qualunque cosa di valore che abbia nell'insieme un valore che raggiunga o superi i 1.000 $ durante tale periodo;

(3) con conoscenza e con l'intento di frodare possieda 15 o più strumenti che siano contraffatti o che siano strumenti di accesso non autorizzati; o

(4) con conoscenza, e con l'intento di frodare, produca, traffichi con, abbia il controllo o la custodia di o possieda attrezzature per realizzare strumenti di accesso;

dovrà, se il reato riguarda il commercio federale o con l'estero, essere punito come previsto nella sottosezione (c) di questa sezione.

(b) (1) Chiunque tenti di commettere un reato previsto nella sottosezione (a) di questa sezione dovrà essere punito come previsto nella sottosezione (c) di questa sezione.

(2) Chiunque concorra con due o più persone ad un progetto criminoso per commettere un reato previsto nella sottosezione (a) di questa sezione, se una delle parti s'impegna in un qualsiasi comportamento per la realizzazione di tale reato, dovrà essere punito con una pena pecuniaria non superiore all'importo previsto come massima pena per tale reato nella sottosezione (c) di questa sezione o imprigionato non più a lungo di metà del periodo previsto come massima pena detentiva per tale reato nella sottosezione (c) di questa sezione, o entrambe.

(c) La pena per un reato previsto nella sottosezione (a) o (b) (1) di questa sezione è —

(1) una pena pecuniaria non superiore all'importo di 10.000 dollari o il doppio del valore ottenuto dal reato oppure una pena detentiva non superiore a 10 anni, o entrambe, nel caso di un reato previsto nella sottosezione (a) (2) o (a) (3) di questa sezione che non avvenga dopo una reclusione per un altro reato nei casi previsti da tale sottosezione, o un tentativo di commettere un reato punibile ai sensi di questo paragrafo;

(2) una pena pecuniaria non superiore all'importo di 50.000 dollari o il doppio del valore ottenuto dal reato oppure una pena detentiva non superiore a 15 anni, o entrambe, nel caso di un reato previsto nella sottosezione (a) (1) o (a) (4) di questa sezione che non avven-

ga dopo una reclusione per un altro reato nei casi previsti da tale sottosezione, o un tentativo di commettere un reato punibile ai sensi di questo paragrafo; e

(3) una pena pecuniaria non superiore all'importo di 100.000 dollari o il doppio del valore ottenuto dal reato oppure una pena detentiva non superiore a 20 anni, o entrambe, nel caso di un reato previsto nella sottosezione (a) di questa sezione che avvenga dopo una reclusione per un altro reato previsto in tale sottosezione, o un tentativo di commettere un reato punibile ai sensi di questo paragrafo.

(d) Il Servizio Segreto degli Stati Uniti avrà, in aggiunta ad ogni altro organismo avente tale potere, l'autorità di indagare sui reati previsti in questa sezione. Tale autorità del Servizio Segreto degli Stati Uniti dovrà essere esercitata secondo le modalità stabilite in un accordo che dovrà tenersi tra il Segretario del Tesoro e il *General Attorney*.

(e) Termini usati in questa sezione —

(1) il termine "strumento di accesso" comprende ogni carta, targhetta, codice, numero di conto, o altri mezzi di accesso al conto che possono essere usati, da soli o insieme ad altri strumenti di accesso, per ottenere denaro, beni, servizi e qualunque altra cosa di valore, o che possono essere usati per iniziare un trasferimento elettronico di fondi (esclusi quelli originati solamente da uno strumento cartaceo);

(2) il termine "strumento di accesso contraffatto" comprende ogni strumento di accesso che sia contraffatto, fittizio, alterato, o falsificato, o un identificabile componente di uno strumento di accesso o di un contraffatto strumento di accesso;

(3) il termine "strumento di accesso non autorizzato" comprende ogni strumento di accesso che sia perso, rubato, scaduto, revocato, cancellato od ottenuto con l'intento di frodare;

(4) il termine "produrre" include disegnare, alterare, autenticare, duplicare, o assemblare;

(5) il termine "trafficare" comprende trasferire o comunque disporre da ad un altro, od ottenere il controllo con l'intento di trasferire o disporre di; e

(6) il termine "attrezzatura per realizzare strumenti di accesso" comprende ogni attrezzatura, meccanismo, o stampigliatura disegnata o principalmente usata per la costruzione di uno strumento di accesso o di uno strumento di accesso contraffatto.

(f) Questa sezione non proibisce qualsiasi attività legalmente autorizzata d'investigazione, protezione, o spionaggio di un organismo degli Stati Uniti a ciò tenuto per legge, di uno Stato, o di una sottodivisione di uno Stato, o di una agenzia di spionaggio degli Stati Uniti, o qualsiasi attività autorizzata ai sensi del titolo V dell'*Organized Crime Control Act* del 1970 (18 U.S.C. *note prec.* 3481).

(b) La tavola delle sezioni all'inizio del capitolo 47 del titolo 18 del codice degli Stati Uniti è modificata con l'aggiunta alla fine del seguente rigo;

1029. — Frode e attività connesse in relazione ai sistemi di accesso ».

Sezione 1603. — Il *General Attorney* dovrà riferire al Congresso annualmente, durante i primi 3 anni seguenti la data di promulgazione di questa legge, sui procedimenti penali in corso relativi a questa sezione del titolo 18 del Codice degli Stati Uniti aggiunto da questo capitolo.