LORENZO PICOTTI

PROBLEMI PENALISTICI IN TEMA DI FALSIFICAZIONE DI DATI INFORMATICI

SOMMARIO 1. Premessa: attualità di indagini penalistiche sulla criminalità informatica. — 2. Le « manipolazioni elettroniche »: distinzioni empiriche e proposte di classificazione. — 3. Documento e « documentazione elettronica » nel nostro ordinamento. — 4. Reati contro la fede pubblica e « manipolazioni elettroniche »: *a*) cenni preliminari; *b*) falsità documentali; *c*) altre falsità. — 5. La nuova fattispecie di « falso in dati memorizzati » nel progetto di una seconda legge per la lotta contro la criminalità economica in discussione nella Repubblica federale di Germania. — 6. Considerazioni conclusive.

1. Un tema di attualità, che emerge a proposito dei reati di falso, concerne la disciplina penalistica delle « falsificazioni » aventi ad oggetto informazioni o più genericamente « dati » destinati a ovvero risultanti da un processo di elaborazione elettronica (od automatica) degli stessi.

L'argomento è meno avveniristico di quanto possa sembrare a prima vista, considerando cioè, soltanto, l'assai scarso interesse dimostrato fino ad oggi dalla dottrina penale italiana per questa problematica[1].

Il costante sviluppo applicativo delle nuove tecnologie informatiche anche nel nostro paese, non solo nella gestione *interna* di imprese

[1] Più in generale scarsa attenzione è stata finora dedicata dalla nostra dottrina al « diritto penale dell'informatica ». Solo recentemente si registrano isolati contributi, aventi peraltro ancora un carattere soprattutto « ricognitivo »: cfr. SARZANA, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1984, I, 21; TRIA, *Osservazioni in tema di « reati elettronici »*, in *Arch. pen.*, 1984, 283; nonché i precedenti lavori dello stesso SARZANA, *Criminalità e tecnologia: il caso dei computer-crimes*, in *Rass. penit. e crim.*, 1979, 53; ID., *Aspetti penalistici e criminologici dei « computer-crimes »*, in *Il diritto dell'informatica: problemi e prospettive* (atti dell'incontro di studio e documentazione per i Magistrati « Vittorio Bachelet » - Siracusa, 6-10 dicembre 1982), Roma, 1983, 41, che con un approccio prevalentemente criminologico (cfr. *ivi*, 45), riporta ampiamente la casistica e le classificazioni ricorrenti nella letteratura straniera, soprattutto nord-americana.

Un sintetico quadro in lingua italiana della ricca tematica penalistica dibattuta nell'ordinamento tedesco-federale è offerto di recente da TIEDEMANN, *Criminalità da « computer »*, in *Pol. dir.*, 1984, 616 (trad. ed appendice a cura di Picotti); mentre con prevalente riferimento alla situazione dell'ordinamento belga si veda SPREUTELS, *La responsabilità penale connessa ad abusi nella applicazione dell'informatica* (trad., a cura di Rossello, del testo della Relazione presentata al Colloquio internazionale « Informatique et Droit en Europe » - Bruxelles, 14-16 giugno 1984), in questa *Rivista*, 1985, 123.

(soprattutto bancarie ed assicurative) e di settori importanti della P.A.[2], ma anche direttamente nei rapporti *esterni* con il pubblico degli utenti e dei fruitori degli ormai numerosi servizi « computerizzati »[3], indica infatti chiaramente che esistono oggi in Italia le condizioni strutturali perché — come insegna l'esperienza delle nazioni più industrializzate — il fenomeno della cosiddetta « criminalità da *computer* » ovvero « informatica »[4] venga a porsi come questione di grande rilevanza sociale ed economica, il cui alto grado di diffusività, dannosità e pericolosità[5] rende necessaria una tempestiva ed adeguata risposta da parte del legislatore e degli organi giudiziari ed inquirenti; nonché consapevoli e specifiche ricerche da parte del sociologo, del criminologo e, non da ultimo, del penalista.

[2] Sul significato e l'ampiezza di tali processi si veda per tutti, da ultimo, il bel volume a cura di RUBERTI, *Tecnologia domani. Utopie differite e transizione in atto*, Bari, 1985, che raccoglie contributi di specialisti di diverse discipline. Oltre al più recente intervento di LOSANO, *Diritto e informatica*, *ivi* pubblicato, 259 ss., per i diversi riflessi di tale sviluppo tecnologico sull'ordinamento giuridico si veda anche GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984 (in specie, sull'automazione degli uffici giudiziari, 126 s.), cui si rinvia per ulteriori riferimenti bibliografici; nonché NOVELLI, *Informatica e pubblica amministrazione*, in *Il diritto dell'informatica: problemi e prospettive*, cit., p. 73 s. Con riferimento specifico alle problematiche connesse con il processo penale, si veda di recente anche RUSSO, *Informatica e criminalità*, in *Riv. it. dir. proc. pen.*, 1984, 324, che riferisce sulla tavola rotonda organizzata a Palermo il 4 febbraio 1984, mentre da ultimo va segnalata anche la raccolta di testi normativi e disposizioni comunitarie curata da D. LIMONE, *Codice dell'informatica*, Rimini, 1985.

[3] L'importanza di tale tendenza ad un'estensione dell'uso o dell'accesso diretto ai sistemi elettronici, che gestiscono servizi di varia natura, da parte degli stessi utenti e clienti « estranei » all'amministrazione od all'impresa che li conduce, con particolare riferimento alla diffusione dei sistemi *videotex* interattivi, è ben sottolineata di recente da SIEBER, *Informationstechnologie und Strafrechtsreform. Zur Reichweite des Künstigen Zweiten Gesetzes, zur Bekämpfung der Wirtschaftskriminalität*,Köln, Berlin, Bonn, München, 1985, 15 s. e 21 s.

[4] La prima locuzione rende, letteralmente, l'espressione originaria di lingua inglese *computer-crime*, ripresa nella letteratura tedesca con il termine *Computer-Kriminalität*; la seconda traduce invece quella francese *Criminalilé informatique*.

Sotto il profilo contenutistico ci sembrano definizioni sostanzialmente equivalenti fra loro, anche se la seconda appare forse più idonea a riabbracciare, con la necessaria latitudine, i diversi fenomeni criminosi connessi non solo con l'uso dei *computers* in senso stretto, ma anche dei « sistemi informatici » in genere. Entrambe tali espressioni ci paiono comunque preferibili a quella ulteriore « criminalità elettronica », con le corrispondenti locuzioni « reato *elettronico* », « moneta *elettronica* », ecc., proposte di recente nella dottrina italiana (cfr. TRIA, cit., p. 283 s. e 286 s.). Tali ultime aggettivazioni paiono infatti troppo strettamente legate a nozioni proprie di una determinata forma tecnologica, e perciò meno consone a definire invece concetti più generali di natura anche sociologica, economica o giuridica, aventi un nesso soltanto mediato e in parte superabile con la prima.

[5] Le dimensioni effettive di diffusione del fenomeno sono in gran parte occultate dalla straordinaria ampiezza della sua « cifra oscura », valutata negli Stati Uniti — richiamando dati della F.B.I. — nell'ordine di 1 caso scoperto ogni 100; mentre soltanto 14 casi, sui 100 scoperti, sarebbero portati poi effettivamente a conoscenza delle autorità inquirenti (BECKER, *The Investigation of Computer Crime*, 1980, 6, 43; cit. in SIEBER, *ComputerKriminalität und Strafrecht*, Köln (2ª ed.), 1981, 2/130).

Altre fonti tedesche oscillano, nella valutazione, fra 4 e 100 casi non scoperti per ogni caso noto (cfr. LENCKNER, *ComputerKriminalität und Vermögensdelikte*, Heidelberg, 1981, 10; e — non senza un'ombra di ironia — STEINKE, *Kriminalität durch Beeinflussung von Rechnerabläufen*, *NStZ*, 1984, 297, con ulteriori richiami).

Anche se pare difficile una precisa valutazione quantitativa del fenomeno, esso è sicuramente consistente, innanzitutto per le « strutturali » difficoltà di natura tecnica che incontra il relativo accertamento, poi

Come vedremo nella presente indagine, le ragioni di interesse per tale argomento sono anche di ordine prettamente teorico: la sempre maggior « astrazione » dei rapporti economico-sociali, che si correla alla applicazione sistematica della tecnologia informatica, per ora soprattutto in significativi momenti della « circolazione » del denaro, mette in discussione infatti alcune nozioni e categorie tradizionali del diritto penale, il cui substrato « naturalistico » è costituito da oggetti materiali, quali ad es. la « cosa mobile » per le fattispecie a tutela del patrimonio od il « documento », per i reati di falso, che qui più direttamente ci interessano.

2. Nell'ambito delle classificazioni generali dei comportamenti « criminali » ovvero « socialmente dannosi »[6] che hanno per oggetto o per « strumento » caratterizzante un'elaborazione elettronica di dati[7],

per la intrinseca contraddittorietà, rispetto alle esigenze di economizzazione dei costi e dei tempi che si perseguono con l'introduzione dei sistemi elettronici, di controlli troppo analitici sulle numerosissime operazioni compiute in tempi assai brevi.

Infine, va segnalata la chiara propensione delle « vittime » a non sporgere denuncia, cercando piuttosto risposta *all'interno* dell'azienda, per evitare il maggior danno al proprio buon nome che deriverebbe dalla cattiva pubblicità del processo penale, che appare per di più spesso di ostacolo alla stessa possibilità di ottenere effettivo risarcimento, una volta che il reo sia condannato e privato di lavoro.

Sull'entità particolarmente elevata dei danni che anche singoli episodi sono in grado di cagionare, sfruttando appunto la caratteristica concentrazione (temporale e spaziale) dei dati nonché automazione dei meccanismi decisionali gestiti dagli elaboratori, si veda per tutti, ampiamente, SIEBER, *Computer Kriminalität*, cit., 140 s. e 2/130 s.

In Italia, per la prima grossa truffa al sistema Bancomat (novembre 1984), i giornali hanno parlato di danni superiori ai 300 milioni di lire (*La Repubblica*, 6 dicembre 1984); mentre per un successivo episodio (aprile 1985) si è riferito di prelievi « abusivi » per un ammontare di 500 milioni di lire (*La Repubblica*, 12 aprile 1985). Anche nel caso di aggressioni non patrimoniali, la particolare pericolosità di questo tipo di delinquenza appare connessa « strutturalmente » all'importanza stessa dei settori e centri decisionali in cui vengono introdotti i sistemi elettronici: siano essi di natura militare, politica od economica.

[6] Occupandosi, ogni ricerca sulla « criminalità da *computer* », (anche) dell'idoneità delle fattispecie del diritto penale positivo a riabbracciare comportamenti e fatti che si presentano almeno in parte come « nuovi », è evidente che la stessa definizione dell'oggetto d'indagine dovrà essere in corrispondente misura « autonoma » dal requisito della concreta « punibilità » (*Strafbarkeit*) o meno dei fatti stessi alla stregua dell'ordinamento vigente. L'indagine dovrà invece orientarsi consapevolmente anche a valutazioni « pre-positive » di dannosità sociale o, meglio, meritevolezza di tutela penale (*Strafwürdigkeit*) dei fatti dannosi manifestatisi nella realtà. La considerazione empirica dei comportamenti da studiare costituisce così il punto di avvio della indagine del penalista, il quale dovrà però poi tenere come parametro di riferimento delle proprie *valutazioni* quelle già ricavabili (anche per analogia) dall'ordinamento positivo: in tal senso cfr. incisivamente LAMPE, *Die strafrechtliche Behandlung der sog. ComputerKriminalität*, *GA*, 1975, 1.

[7] Nell'ambito della dibattuta questione definitoria del concetto stesso di criminalità informatica, su cui non intendiamo ovviamente prendere posizione in questa sede, il riferimento al « processo di elaborazione » anziché all'« elaboratore », che può essere inteso anche solo nella sua materialità (c.d. *hardware*) ci sembra un elemento importante per selezionare, fra i diversi problemi, quelli effettivamente nuovi, indotti dall'introduzione delle tecnologie elettroniche, rispetto a quelli che costituiscono invece mera riproposizione o rilettura di tradizionali questioni o fattispecie alla luce soltanto del particolare oggetto materiale costituito dal « calcolatore elettronico » (o da sue parti).

Pur potendo avere una rilevanza sul piano della indagine criminologica ovvero an-

e per la cui riuscita, da un lato, e scoperta, dall'altro, appare come condizione essenziale la conoscenza specifica della tecnologia del *computer*[8], la presente indagine si limiterà a considerare quelle sole condotte, definite comunemente come « manipolazioni informatiche », che costituiscono la più diffusa ed importante forma di mani-

che della tecnica legislativa o della politica sanzionatoria, una estensione del concetto di « criminalità informatica » a tutti i comportamenti criminali comunque « connessi » col *computer*, nella sua eccezione più ampia, non giustifica a nostro avviso una autonomia scientifica dell'oggetto d'indagine, quantomeno per il diritto penale.

Così, nell'ordinamento italiano, il « nuovo » art. 420 cod. pen. (introdotto con l'art. 1 del d.l. 21 marzo 1978, n. 59, convertito con modificazioni nella legge 18 maggio 1978, n. 191), che punisce gli « attentati a impianti di pubblica utilità » annoverandovi espressamente anche quelli « di elaborazione di dati », non ci pare contribuisca specificamente alla costruzione di un « diritto penale dell'informatica ».

Per una sia pure generica distinzione fra una concezione « ampia » di « diritto penale dell'informatica » (riabbracciante tutti gli illeciti « comunque connessi » all'uso del *computer*) ed una più ristretta, relativa solo a « determinati specifici comportamenti » in tale campo, si veda SARZANA, *Note*, cit. (1), 22 che restringe così quella nozione più generale fornita in un suo primo scritto (ID., *Criminalità e tecnologia*, cit. (1), 59).

Nella dottrina tedesca, superate le posizioni « estreme » di chi negava addirittura l'autonomia se non l'esistenza stessa del problema della « criminalità da *computer* » (cfr. in specie BETZL, *ComputerKriminalität - Dichtung und Wahreit*, *DSWR*, 1972, 317 ss., e la sua polemica, a botta e risposta, con SIEBEN e VON ZUR MÜHLEN, *ComputerKriminalität - nicht Dictung, sondetn Wahreit*, *DSWR*, 1972, 397, ecc. ricordata dettagliatamente da LAMPE, cit. (6), 1, nota (1)), appaiono oggi isolate anche le posizioni di chi non ritiene necessario o urgente un *apposito* intervento legislativo per riabbracciare le nuove condotte che si manifestano in tale campo (cfr. in tal senso da ultimo STEINKE, cit. (5), 295, nocnhé TRÖNDLE, *Zum Tatbestand des Computerbetrugs* (Arbeitstagung der StafrechtsKommission des Deutschen Richterbundes, Bamberg, 23-28-4-1979), richiamato da LENCKNER, cit. (5), 25).

Ampia prevalenza hanno invece le posizioni di chi, pur muovendo da nozioni relativamente late e concettualmente indeterminate di « criminalità da *computer* », propugna comunque la necessità di un urgente intervento legislativo, per regolamentare quantomeno i seguenti quattro gruppi principali di comportamenti: le « truffe mediante *computer* », gli spionaggi informatici, i sabotaggi informatici (in cui si ricomprendono anche sabotaggi e danneggiamenti alle parti materiali dei *computers*) e l'uso abusivo dei calcolatori (sia dell'*hardware* che del *software*): così da ultimo SIEBER, *Informationstechnologie*, cit. (3), 14 ss. che riporta la definizione ufficiale, estremamente ampia (« involving » ADP and/or TD) fornita nel maggio 1983 dal gruppo internazionale di esperti dell'O.E.C.D.; e STEINKE, cit. (5), 295, che riporta le definizioni formulate dal competente gruppo di lavoro dell'Ufficio federale tedesco di polizia criminale.

[8] Tale specificazione, per lo più respinta nella letteratura tedesca (cfr. per tutti SIEBER, cit. (5), 188 s.), salvo talune posizioni più problematiche (cfr. LAMPE, cit. (6), 7, nota (2) e LENCKNER, cit. (5), 14 s.), compare invece nella letteratura nordamericana e nella stessa definizione « ufficiale » di *computer-crime* contenuta nel rapporto dell'U.S. DEPARTEMENT OF JUSTICE - National Criminal Justice Information and Statistics Service, *Computer Crime: Criminal Justice Resource Manual*, Washington, 1979, XXVI (cit. da BECKER, *Informatica: aspetti politici e giuridici*, in *Il diritto dell'informatica: problemi e prospettive*, cit. (1), 148).

Tale specificazione, che pur conserva un proprio autonomo significato sostanziale, trae origine dalla prospettiva processualistico-probatoria in cui si è posto inizialmente il problema della criminalità relativa a *computer* nell'ordinamento nordamericano: in particolare dalla questione preliminare della stessa utilizzabilità come prova, ai fini giudiziari — stante il rigoroso sistema legalistico al riguardo vigente — dei dati elettronici e dei riscontri contabili e commerciali forniti tramite elaboratore.

Sul punto si veda ampiamente BEQUAI, *Computer crime*, Lexington, 1978, 128 ss. (cit. da SARZANA, *Criminalità e tecnologia*, cit. (1), 78 s.).

Per una definizione più ampia e generica di *computer-crime* si veda invece PARKER, *Crime by Computer*, New York, 1976, 12, e da ultimo ID., *Fighting Computer Crime*, New York, 1983.

festazione di questo tipo di criminalità[9] e che rappresentano — anche sul piano teorico — il primo momento di verifica dell'applicabilità del diritto penale vigente ai nuovi comportamenti indotti dallo sviluppo tecnologico.

Oltre che nell'esperienza straniera, l'importanza attuale di tali condotte criminose trova verifica nella stessa casistica finora nota in Italia: in particolare, la maggior parte dei comportamenti « infedeli » fino ad oggi scoperti (o perlomeno resi noti) posti in essere all'interno di aziende che utilizzano sistemi informatici[10], come pure dei sempre più frequenti episodi di « truffe » (commesse da « estranei ») a danno dei sistemi automatici di erogazione di denaro contante (cosiddetti sportelli Bancomat)[11], appaiono costituiti precisamente da « manipolazioni » dei processi di elaborazione elettronica.

Per meglio evidenziarne i tratti distintivi, si è soliti distinguere tre diverse possibilità di manipolazione, a seconda che queste vengano poste in essere nella fase di immissione (*input*) ovvero di elaborazione od infine di emissione (*output*) dei dati. Nell'ambito delle manipolazioni che intervengono nella seconda fase, interferendo cioè direttamente sull'elaborazione automatica in senso stretto, si distinguono poi quelle effettuate tramite la *consolle*, da quelle c.d. « di programma »[12], che consistono in una preordinata e « fraudolenta » modifica dello stesso. Queste non vanno confuse con le manipolazioni dell'*input*, che presuppongono l'esistenza di un elaboratore già « programmato », e si realizzano inserendovi, semplicemente, dei dati « falsi », ovvero alterando informazioni vere, od ancora eliminandole in tutto o in parte, o fornendole in collocazione o in momenti sbagliati, al fine di sfruttare poi l'elaborazione « secondo programma » di tali *input* « manipolati ».

Nella letteratura in argomento si cita l'esempio dell'operatore infedele che, fornendo « falsi » dati, relativi a fornitori o dipendenti fittizi di un'impresa, ai quali secondo programma devono essere pagate o accreditate periodicamente somme di denaro, crea, per sé o per i propri complici, disponibilità di denaro (di giro) su conti opportunamente indicati all'elaboratore stesso, che dispone anche i corrispondenti accrediti[13].

Molte ipotesi di « truffa » al sistema Bancomat sono state realizzate in Italia inserendo semplicemente negli sportelli automatici dati

[9] In tal senso si vedano, per tutti, le concordi affermazioni di LAMPE, cit. (6), 2 e SIEBER, cit. (3), 15 nonché ID., *Gefahr und Abwehr der ComputerKriminalität*, *BB*, 1982, 1433, ove si stima che le manipolazioni costituiscano circa il 60% di tutti i reati informatici scoperti nella Repubblica federale.

[10] Per una esemplificazione nella scarsa casistica nota in Italia fino ad ora, cfr. SARZANA, *Criminalità e tecnologia*, cit. (1), 57; nonché TRIA, cit. (1), 283 s. che sottolinea l'importanza dell'estensione dei sistemi di trasferimenti elettronici di fondi (EFT) anche nella realtà bancaria italiana, quale occasione di « reati elettronici ».

[11] Si tratta degli episodi già citati alla nota (5) e su cui si tornerà anche più avanti.

[12] Sul punto si veda LAMPE, cit. (6), 13 s., nonché dettagliatamente, con ricca esposizione casistica, SIEBER, cit. (5), 40 ss. e, per ulteriori ipotesi, 2/97 ss.

[13] Il caso è riportato da ultimo da TIEDEMANN, cit. (1), 616.

identificativi « falsi » — o meglio: relativi ad un cliente vero, ma abusivamente riprodotti su numerosi esemplari « non autentici » di tessere (o carte) a banda magnetica — ed ottenendo poi, « secondo programma », la « consegna » delle somme di denaro contante richieste, ai detentori ed utilizzatori delle carte stesse[14].

Nell'ambito delle « manipolazioni di programma », invece, sono note varie tecniche, le principali delle quali vengono individuate, dalla letteratura nordamericana, nel « cavallo di Troia », che consiste nel piazzamento segreto di istruzioni in programma, in modo tale da far svolgere all'elaboratore delle funzioni non autorizzate, permettendogli però di continuare anche a svolgere le sue funzioni normali; o nelle « tecniche salame », che consentono l'appropriazione di piccoli quantitativi di beni da un gran numero di riserve (ad es. nell'ambito dei sistemi finanziari, col recupero degli « arrotondamenti in perdita ») da accreditare poi tutti su un solo conto[15].

Altre tecniche, solitamente descritte, sono invece meramente strumentali alle vere e proprie manipolazioni, come nel caso del *Superzapping*, che consiste nell'utilizzazione di un programma speciale, c.d. di accesso universale, per superare tutti o determinati controlli e modificare (o rivelare) poi qualsiasi parte del contenuto del *computer*; i c.d. « trabocchetti », che di per sè sono congegni per la ricerca e correzione di errori (c.d. *debugging*) nella fase di programmazione e consistono nella possibilità di interrompere la sequenza di istruzioni del programma, ma sono perciò utilizzabili anche per l'accesso abusivo, la modifica o l'inserimento di nuove istruzioni; le c.d. « bombe logiche », che sono programmi la cui esecuzione ad intervalli appropriati o determinati in un sistema computerizzato ne determina condizioni o stati che consentono o facilitano il compimento di atti non autorizzati o illeciti; ecc.[16].

[14] Per più dettagliati resoconti giornalistici si vedano fra i tanti, oltre a quelli citati alla precedente nota (5), *Il Corriere della Sera* del 6 dicembre 1984 e *Panorama* del 17 dicembre 1984, n.65 s.

[15] Per tali denominazioni, ormai « classiche », si veda U.S. DEPARTEMENT OF JUSTICE, cit. alla nota (8), nonché riassuntivamente, nella letteratura italiana, SARZANA, *Aspetti penalistici*, cit. (1), 59-60; ed ora anche la traduzione di SPREUTELS, cit. (1), 125-126.

[16] Il *Criminal Justice Resource Manual*, a cura dell'U.S. DEPARTEMENT OF JUSTICE, cit. (8), riporta molti altri tradizionali *modi operandi* rilevati nella commissione dei *computer-crimes*, ed ampiamente ripresi anche nella letteratura internazionale in materia (da ultimo si veda la sintesi di BOLAÑOS RAMIREZ, *Computer Crime: a New Legal Concept*, in *Agora*, 1985, I, 26). Ne elenchiamo per completezza alcuni altri, anche se non costituiscono « manipolazioni » di dati o programmi, potendo tutt'al più essere strumentali ad esse: gli « attacchi asincroni » che permettono di violare l'isolamento di un lavoro da un altro; lo « spazzinaggio », che consiste nella ricerca di informazioni « residue », lasciate dopo l'esecuzione di un lavoro; la « fuoriuscita di dati » da un sistema computerizzato previo mascheramento, in blocchi di dati « innocui » o lecitamente richiesti, o in altro modo; il *piggy-backing* e l'« impersonificazione », che consentono di ottenere l'accesso a zone « controllate », sfruttando l'« autorizzazione » contestualmente fornita ad un accesso legittimo, ovvero mediante l'assunzione delle caratteristiche di identificazione di un'altra persona; le « intercettazioni », che possono essere realizzate anche magneticamente, senza necessario collegamento su filo; la « simulazione » e « modello », in cui il *computer* diviene strumento per la stessa progettazione e controllo della riuscita del reato.

Di minor interesse appaiono gli interventi operati direttamente tramite la *consolle*, per impedire o ritardare la registrazione di determinate operazioni, che sarebbero previste nel programma[17], mediante l'inserimento da tastiera di specifiche istruzioni nel linguaggio operativo o di controllo della macchina.

Molto spesso, le manipolazioni di *consolle* come del resto quelle di *input* si combinano con le manipolazioni di programma (e queste fra loro), per meglio neutralizzare od aggirare gli sbarramenti e i sistemi di sicurezza o controllo[18].

A questo insieme di manipolazioni si affiancano infine quelle poste in essere nella terza fase, c.d. di emissione dei dati (o *output*), che intervengono nella stampa o riproduzione visiva o trasmissione dei dati risultanti da un'elaborazone già compiuta « correttamente » per impedirla o modificarla in tutto o in parte. Esse consistono per lo più in interventi « diretti » sulle parti meccaniche dell'elaboratore (stampanti, video, trasmettitori), e rivestono un certo autonomo interesse — quando non si risolvano in manipolazioni di dati destinati ad essere nuovamente sottoposti ad un ulteriore processo di elaborazione, nel qual caso rileveranno come manipolazioni di *input* — soprattutto nel caso di sistemi telematici, che prevedono la trasmissione dei risultati dell'elaborazione a distanza[19]. In tali casi è possibile, infatti, mediante l'inserimento ad esempio su cavi telefonici, utilizzati per la trasmissione dei dati, non solo la loro intercettazione, ma anche una loro autonoma manipolazione.

Per lo più però le manipolazioni dell'*output* non presentano peculiarità specifiche, *interne* alle tecniche di elaborazione elettronica, trattandosi di modificazioni *successive*, relative alla espressione dei suoi risultati, che solo « apparentemente » provengono dal precedente procedimento elettronico stesso.

La maggior pericolosità ed insidiosità delle manipolazioni di *input* e di programma derivano dal fatto che le stesse, una volta impostate con successo, vengono poi « gestite » automaticamente dallo stesso elaboratore elettronico; e non solo possono ripetersi così nel tempo senza bisogno di altri interventi diretti dell'autore (si è parlato in tali casi di una vera e propria « permanenza » del reato)[20], ma soprattutto sono strutturalmente in grado di sfuggire ad ogni ulteriore controllo « a valle ».

[17] Un caso famoso in cui fu applicata una simile tecnica è ricordato da TIEDEMANN, cit. (1), 617.

[18] Come accadde nel caso già sopra citato alla nota (13), in cui il programmatore infedele, per evitare la scoperta dei pagamenti disposti dall'elaboratore a favore di persone fittizie, modificò anche i programmi di stampa delle buste paga, degli elenchi riepilogativi, dei progetti contabili, dei bilanci, ecc.

[19] LAMPE, cit. (6), 17, include peraltro sostanzialmente in tale gruppo anche tutte le manipolazioni tramite *consol.*

Più precisa ci pare la distinzione operata da SIEBER, cit. (9), 1435.

[20] Così SIEBER, cit. (5), 126 ss. e 2/106 ss.; nonché SOLARZ, *Computer Technology and Computer Crime* (Rapporto n. 8 della « Research and Development Division » del « National Swedish Council for Crime Prevention »), Stockholm, 1981, 13 s.

L'autore può anche « programmare » infatti l'autocancellazione delle manipolazioni effettuate, dopo un certo numero di ripetizioni, e non lasciare traccia alcuna delle operazioni illecite compiute. Inoltre, l'affidamento, almeno in una certa misura, nel processo di elaborazione elettronica costituisce un presupposto ineliminabile di ogni utilizzazione applicativa dei sistemi informatici. E la vigilanza dell'uomo sull'enorme numero di operazioni compiute in tempi brevissimi dal *computer* non potrà che essere parziale o meramente « casuale »[21], per non contraddire gli stessi scopi di razionalizzazione ed economizzazione che si perseguono con il suo utilizzo su larga scala. D'altronde, per ragioni tecniche o giuridiche, certi controlli dipendono *solo* da pochi soggetti, aventi piena « signoria » sull'intero sistema di elaborazione elettronica, di cui è precluso il controllo da parte di altri.

Sarà perciò molto probabile che una manipolazione ben congegnata sfugga ad ogni verifica e che il suo risultato non compaia affatto ovvero si presenti come prodotto « autentico » e/o « genuino » della elaborazione programmata.

Inoltre oggi, con lo sviluppo dei sistemi telematici, molte « manipolazioni » non solo possono essere realizzate da operatori, programmatori od addetti infedeli, o comunque da chi acceda legittimamente all'elaborazione; bensì sono eseguibili anche inserendoli « dall'esterno » nel processo di elaborazione, attraverso l'abuso dei possibili terminali destinati al pubblico, ovvero con l'intercettazione delle linee e derivazioni per la trasmissione dei dati a distanza: ed aggirando poi « elettronicamente » i sistemi di sicurezza e controllo che dovrebbero garantire la « legittimità » dell'accesso e dell'uso dell'elaboratore, che difficilmente si dimostrano insuperabili per mani esperte od anche per intraprendenti e creativi appassionati[21-bis].

In primo piano si colloca così, rispetto a molte condotte di manipolazione, il momento dell'*accesso abusivo* all'elaborazione, da intendere non solo come condotta di illegittimo accostamento « materiale » al *computer*, quanto molto più spesso e soprattutto come elusione « elettronica » delle misure di sicurezza che la stessa tecnica informatica e di programmazione impone, quali la « identificazione » dell'operatore, la « autenticazione » della sua identità, l'autorizzazione e quindi la registrazione dell'accesso richiesto[22]; nonché il controllo « interno » sulla regolare sequenza ed utilizzazione delle divere operazioni in cui si articola lo svolgimento del programma.

[21] Ciò è del resto ampiamente confermato dall'esperienza internazionale fino ad oggi: cfr. per tutti SIEBER, cit. (5), 146 ss.; WHITESIDE, *Computer Capers*, New York, 1978, 59 s.

[21-bis] Cfr., per una rassegna di « casi celebri », SPREUTELS, cit. (1), 126-127.

[22] Per un sintetico ma significativo quadro di tali questioni si veda, nella letteratura italiana, BUCCIARELLI, *I problemi della sicurezza*, in *Tesi e proposte normative per la società dell'informazione: dal diritto d'autore alla* deregulation (Atti delle giornate di studio dell'ANFoV - Torino, 19-20 ottobre 1983), Torino, 1984, 115-120.

Oltre alla tradizionale distinzione operata in dottrina e sopra esposta, fra le diverse fasi in cui possono intervenire le manipolazioni, può essere allora importante — ai fini di un significativo inquadramento giuridico-penale — evidenziare altresì la distinzione fra manipolazioni « in senso stretto » di dati o programmi informatici (genericamente considerati nel loro *contenuto*); e « falsificazioni » od operazioni « fraudolente », in qualunque « fase » realizzate, *strumentalmente* dirette solo a consentire l'accesso al o l'utilizzo « abusivo » del processo di elaborazione: avvengano esse per operare successive manipolazioni « in senso stretto », ovvero anche « semplicemente » per procurare all'autore la conoscenza (o l'eventuale successiva rivelazione o riproduzione « abusiva ») dei dati, delle informazioni, o dei programmi stessi[23]; od infine anche solo per utilizzare, senza costo alcuno, elaboratori e programmi altrui[24].

In contrapposizione a tale gruppo di condotte, « abusive » già alla stregua delle regole interne del sistema informatico, ed aggressive solitamente degli interessi e diritti del *titolare legittimo* del processo di elaborazione (fra le quali dobbiamo includere non solo quelle realizzate dall'*esterno*, ma anche quelle poste in essere all'*interno* di enti o società, da parte di singoli amministratori, dirigenti od operatori infedeli, a danno dell'interesse stesso dell'ente o della società), si debbono collocare quelle altre imputabili (direttamente od indirettamente) al « titolare » e compiute a danno degli interessi degli *utenti* o dei *terzi* che si avvalgono del o si affidano al sistema informatico.

Limitandoci qui ad una esemplificazione banale, possiamo pensare alle « frodi fiscali », eseguibilida imprese commerciali mediante programmi di registrazione solo parziale delle operazioni effettuate, in violazione ad es. della recente normativa sui registratori di cassa; oppure alle « appropriazioni » che possono essere realizzate dalle aziende di credito, mediante programmi che « ritardino » o riducano addirittura gli accrediti dei correntisti od « anticipino » l'addebito di valuta dei prelievi da costoro effettuati agli sportelli automatici (nor-

[23] In tali ipotesi le manipolazioni sarebbero strumentali al c.d. spionaggio informatico, che costituisce l'altra forma più rilevante in cui si è manifestata finora la criminalità informatica.

In tale settore le manipolazioni (strumentali) rappresentano però solo una (sia pure frequente) eventualità, mentre i più gravi problemi sorgono a proposito della qualificazione stessa del *software* quale possibile oggetto di tutela, ai sensi della normativa sul diritto d'autore ovvero di quella sui brevetti o sul segreto industriale.

L'insieme di tali questioni costituisce perciò un autonomo campo di studio e ricerca, di pertinenza del civilista oltreché del penalista, e rispetto al quale si registra finora un'ampia produzione dottrinale ed anche giurisprudenziale: per le principali indicazioni al riguardo relative al nostro ordinamento, cfr. PICOTTI, *Appendice* al saggio di TIEDEMANN, cit. (1), 637-639.

[24] In tal modo potrebbe forse risolversi la discussa questione se sia di per sé punibile, o se sia comunque meritevole di autonoma previsione penale, il c.d. « furto di tempo » (*Zeitdiebstahl*), consistente nell'utilizzazione non autorizzata di un cervello elettronico: ove infatti non integri già altri reati (furto di energia elettrica, ad. es.), lo stesso potrebbe essere sanzionato nei limiti in cui comporti il ricorso ad un mezzo « fraudolento » per ottenere l'autorizzazione all'accesso: in analoga prospettiva ci pare si collochi TIEDEMANN, cit. (1), 622, che pur non giunge ad una precisa presa di posizione; mentre SIEBER, cit. (3), 46, insiste da ultimo per la creazione di una specifica norma penale.

malmente, peraltro, le condizioni contrattuali accettate dal cliente non vincolano la banca al rispetto di termini tassativi ed autorizzano anzi espressamente simili condotte); od infine, più in generale, alla creazione di scritture o documentazioni contabile falsa o fittizia, come si verificò nella famosa frode posta in essere da una Compagnia di assicurazione nord-americana, che rivendette ad altre Compagnie migliaia di polizze fittizie, fornendo la sola « documentazione » prodotta dall'elaboratore con un apposito programma, che modificava i dati di vecchie polizze, ormai estinte[24-bis].

La peculiarità di tale secondo gruppo di condotte ci pare costituita dal fatto che le stesse non presuppongono l'« abuso » dell'*accesso* o dell'*utilizzo* dell'elaborazione, alla stregua del suo programma e delle sue misure di sicurezza.

Tuttavia le stesse devono egualmente considerarsi come « manipolazioni informatiche » poiché da un lato appaiono realizzabili tipicamente solo attraverso l'elaborazione elettronica, e dall'altro il programma predisposto — sia pure in modo *non* abusivo nel senso sopra specificato — prevede però una mancanza di corrispondenza fra il contenuto delle registrazioni ed elaborazioni da effettuare, aventi efficacia « probatoria » nei rapporti con gli utenti od i terzi, e la reale dimensione delle operazioni effettuate, oggetto dell'*input*, quali riportate ad esempio a stampa sugli « scontrini » o pro-memoria rilasciati automaticamente agli utenti od ai terzi dall'elaboratore, ma sforniti di per sé di valore « probatorio ».

3. Le descritte possibilità di « manipolazione » dei dati informatici pongono in primo piano il più generale problema del valore giuridico da riconoscere (anche ai fini della tutela penale che in questa sede ci interessa) alla « documentazione elettronica », vale a dire alla documentazione (intesa in senso lato) frutto od oggetto di elaborazione automatica da parte dei moderni mezzi dell'informatica[25]: sia essa o meno prodotta su supporti cartacei ovvero in « linguaggio » leggibile dall'uomo.

Come è noto, l'ordinamento giuridico ha tradizionalmente identificato la nozione di « documento » con quella di « documento scritto » ed in specie « cartaeco », anche se da tempo la dottrina ha evidenziato l'autonomia del *concetto* di « documento », inteso in senso ampio, e ravvisabile in « qualunque cosa idonea alla *rappresentazione* di un fatto »[26], destinabile e idonea a fini probatori[27], da quello di « documento scritto », che ne costituisce solo una specie.

[24-bis] Cfr. per l'esposizione di tale caso in lingua italiana SARZANA, *Criminalità e tecnologia*, cit. (1), 72/74.

[25] Cfr. per una definizione analoga GIANNANTONIO, cit. (2), 148.

[26] CARNELUTTI, *Teoria del falso*, Padova, 1935, 139 (corsivo nostro); nonché ID., *Documento (teoria moderna)*, in *Noviss. Dig. it.*, VI, Torino, 1968, 86.

[27] La precisazione, che riflette una prospettiva processuale-probatoria in tema di reati contro la fede pubblica, è di MALINVERNI, *Teoria del falso documentale*, Milano, 1958, 267. Analogamente anche CRISTIANI, *Fede pubblica (delitti contro la)*, in *Noviss. Dig. it.*, VII, Torino, 1968, 176.

Nell'ambito della nozione di genere trova infatti già espressa rilevanza giuridica il diverso concetto di « contrassegno », che prescinde appunto dal requisito della « scritturazione »[28].

L'attuale disciplina legislativa considera peraltro come del tutto marginali le forme di « documentazione » diverse da quella scritta.

Il codice civile limita le sue previsioni al riguardo alle obsolete « tagli e tacche di contrassegno » (art. 2713 cod. civ.), mentre alle « riproduzioni meccaniche » (fotografiche, cinematografiche, fonografiche e di « ogni » altra specie: art. 2712 cod. civ.) riconosce una efficacia probatoria condizionata al mancato disconoscimento del controinteressato (salva, per le sole « copie fotografiche di scritture » (art. 2719 cod. civ.), la possibilità di attestazione di « conformità » con l'originale da parte di un pubblico ufficiale).

La più recente legge 4 gennaio 1968, contenente « Norme sulla documentazione ed autenticazione di firme », consente invero alla P.A. di sostituire *a tutti gli effetti* (art. 25) i « documenti » dei propri archivi con la corrispondente documentazione microfilmata, secondo formalità prescritte da apposito regolamento[29].

In tal modo viene eroso il tradizionale principio, secondo cui l'atto pubblico, sia esso il documento originale ovvero un pubblico certificato, dovrebbe sempre essere esternato in forma scritta[30], intesa come rappresentazione grafico-alfabetica su un supporto cartaceo.

Con apposite norme oggi è consentito anche il rilascio di certificati (ad es. anagrafici o di casellario giudiziario) sotto forma di tabulati, prodotti da un sistema elettronico: anche se non può prescindersi, ai fini della loro efficacia probatoria, dalle formalità descritte dagli artt. 12 e 13 della citata legge 15/1968, in particolare dalla sottoscrizione da parte del soggetto che li « emana ».

L'atto pubblico originario od un pubblico registro non possono infatti ancora essere costituiti *solo*, o sostituiti integralmente, da un sistema informatico[31].

Ma con apposite norme di legge si sta introducendo espressamente proprio tale possibilità; in specie, la recente riforma delle Conservatorie dei registri immobiliari, che ne prevede la « meccanizzazione » mediante l'uso di elaboratori elettronici, stabilisce che in futuro la stessa presentazione delle note di trascrizione avvenga direttamente

[28] Cfr. già BINDING, *Lehrbuch des gemeinen deutschen Strafrechts*, Bes.T., Leipzig, vol. II (2ª ed.), 1904, 170 s.; CARNELUTTI, *Teoria*, cit. (26), 9 e 170; e MALINVERNI, cit. (27), 24 s. e 81 s., il quale sottolinea come tale categoria (accolta nel cod. civ. agli artt. 2712 e 2713) sia destinata ad ampliare e ad acquisire crescente importanza, evolvendosi in sintonia con lo sviluppo tecnologico (95 s.).

[29] Sul punto si veda diffusamente GIANNANTONIO, cit. (2), 156 s.

[30] Sul concetto di scrittura, come rappresentazione « alfabetica » e non « ideografica », caratterizzata non solo dalla struttura o natura del « simbolo » utilizzato, ma anche e soprattutto dalla appartenenza di esso ad un sistema di regole che ne definisce funzione e ruolo, così da costituire un « linguaggio », si veda, oltre a MALINVERNI, cit. (27), 81 ss. (nonché ID., *Ai limiti tra le scritture e i contrassegni*, in *Scuola pos.*, 1964, 89) di recente — con alcune precisazioni — NAPPI, *I delitti contro la fede pubblica*, in BRICOLA, ZAGREBELSKY (a cura di), *Codice penale, Parte speciale*, vol. I, Torino, 1984, 618.

[31] Cfr. GIANNANTONIO, cit. (2), 155.

su « supporti informatici » e che la loro trasmissione si effettui mediante elaboratori elettronici[32].

La normativa in materia di accertamento delle imposte sui redditi delle persone fisiche e giuridiche (art. 14, comma 3, d.P.R. 29 settembre 1973, n. 600) del resto autorizza e disciplina da tempo l'utilizzo della documentazione elettronica (o microfilmata) nel campo delle scritture obbligatorie ai fini fiscali.

Peraltro, la loro efficacia probatoria presuppone sempre una previa annotazione cartacea e poi la stampa, in linguaggio leggibile all'uomo, della stessa elaborazione su supporti cartacei o pellicole fotografiche.

La necessità della « forma scritta » (quale presupposto della efficacia probatoria del documento, inteso in senso stretto), discende anche dalle norme civilistiche in tema di telegramma (artt. 2705-2706 cod. civ.).

In ragione della sua peculiare tecnica di comunicazione, questo può però prescindere dal requisito, solitamente richiesto nel campo delle « scritture private », della *sottoscrizione* autografa (art. 2702 cod. civ.) da parte dell'autore[33].

In definitiva, ci pare che un pur sintetico quadro della nozione e della disciplina extrapenale del concetto di « documento » evidenzi una situazione assai meno uniforme e statica di quanto si possa pensare.

Soprattutto, emerge una naturale tendenza all'adattamento alle nuove tecniche di comunicazione e, quindi, di informazione, che pur con le lentezze e le difficoltà specificamente connaturate alla funzione « probatoria » propria della stessa idea di « documentazione » intesa in senso lato (cristallizzatrice, per così dire, dei rapporti sociali in funzione della loro « certezza »), dimostra il carattere *normativo*, e perciò in costante evoluzione, della categoria.

Non ci pare dunque azzardato né prematuro, seguendo indicazioni tratte dall'esperienza straniera[34], verificare fin d'ora le possibilità di inquadramento delle « manipolazioni informatiche » nell'ambito delle fattispecie poste a tutela della « fede pubblica ».

[32] Si tratta della legge 27 febbraio 1985, n. 52 (in *G.U.*, 6 marzo 1985, n. 56), il cui disegno trovasi pubblicato già in « Appendice » a GIANNANTONIO, cit. (2), 318 ss., assieme, fra l'altro, al c.d. « progetto Novelli » sulla disciplina generale dell'utilizzazione, da parte dell'amministrazione dello Stato, di sistemi di trattamento automatico di dati e di informazioni (*ivi*, 308 s.).

[33] Anche le scritture contabili delle imprese (artt. 2709-2710 cod. civ.), come del resto le carte e i registri domestici (art. 2707 cod. civ.) e le « annotazioni » su documenti (art. 2708 cod. civ.) hanno valore probatorio pur in mancanza della sottoscrizione dell'autore (che peraltro deve sempre essere sicuramente identificabile *aliunde*), in ragione e limitatamente allo specifico tipo di rapporto sottostante cui si riferiscono.

[34] Soprattutto la dottrina tedesca ha fin da subito collocato la tematica delle « manipolazioni » nel campo delle falsità punibili (o quantomeno « meritevoli » di pena): cfr. per tutti LAMPE, cit. (6), 2 ss.; ed ora riassuntivamente SIEBER, cit. (3), 25 s., che riprende l'ampio dibattito sviluppatosi in Germania ed ancora in corso, avente ad oggetto anche le proposte di riforma del codice penale di cui meglio si dirà al successivo paragrafo.

4. *a*) Le manipolazioni informatiche finora note, pur essendosi indirizzate o risolte prevalentemente in aggressioni al patrimonio altrui, non paiono riducibili sistematicamente (come pure è stato in un primo tempo proposto) a semplici forme di manifestazione dei reati contro il patrimonio[35] o contro l'economia[36].

Innanzitutto, manipolazioni di dati e programmi elettronici sono state accertate anche a danno di elaboratori di enti pubblici, che gestivano, ad es., programmi di assistenza sociale, ovvero di Università, che memorizzavano i risultati di esami e valutazioni degli studenti, nonché di laboratori di analisi, che dovevano accertare la percentuale di alcool presente nel sangue di conducenti sorpresi in presunto stato di ebrezza[37].

In secondo luogo, proprio il carattere « strumentale », rispetto all'aggressione di ulteriori e diversi *beni giuridici*, che le manipolazioni informatiche solitamente presentano, costituisce elemento di marcato parallelismo con le condotte riconducibili ai delitti contro la « fede pubblica » in genere[38]: proprio l'« evanescente » o proteiforme oggettività giuridica che si esprime in tale discusso concetto, consente di riferirvi — almeno in ipotesi — anche forme di aggressione nuove o del tutto diverse da quelle tradizionali.

Un forte argomento di politica del diritto, a favore dell'applicazione di tali norme, è stato indicato anche nel fatto che esse potrebbero garantire una significativa « anticipazione » della stessa soglia di tutela penale, rispetto alla causazione di danni od al conseguimento « fraudolento » di vantaggi (per lo più patrimoniali) ingiusti, la cui effettiva realizzazione segna invece il momento consumativo di molti reati contro il patrimonio[39].

[35] In tal senso cfr. la prima edizione del lavoro di SIEBER, cit. (5), 188; nonché TIEDEMANN, cit. (1), 615.

[36] In questa prospettiva pare orientata molta dottrina penalistica, oltreché criminologica: in specie cfr. TIEDEMENN, *Wirtschaftstrafrecht und Wirtschaftskriminalität*; KAISER, *Criminologia* (trad. id. a cura di Morselli e Blonk Steiner, Milano, 1985, 353; nonché, per quella italiana, SARZANA, *Criminalità e tecnologia*, cit. (1), 56.

Che il tema sia comunque strettamente collegato a quello della criminalità economica, è dimostrato dal fatto che nella stessa Repubblica federale di Germania i relativi progetti di riforma — concernenti anche i reati di falso — sono previsti bell'ambito del disegno di una seconda legge per la lotta contro la criminalità economica (2. WiKG), ed affidata perciò all'elaborazione della relativa commissione d'esperti (sul punto si tornerà nel successivi par. 5).

[37] Cfr., per tali esemplificazioni, LENCKNER, cit. (1), 13, che critica infatti i citati orientamenti della dottrina.

[38] Sul punto concordano le posizioni non solo di chi muove da una concezione « necessariamente » plurioffensiva dei reati contro la fede pubblica (per tutti cfr. ANTOLISEI, *Sull'essenza dei delitti contro la fede pubblica*, in *Studi in memoria di Arturo Rocco*, Milano, 1952, 95 ss.; nonché ID., *Manuale di diritto penale, Parte speciale*, vol. II, Milano, 1966, 489 ss.); ma anche di chi sostiene concezioni c.d. « processual-probatorie »: cfr. per tutti MALINVERNI, cit. (27), 162 (con ampia ricostruzione storica).

[39] Del resto, la stessa applicazione delle comuni fattispecie contro il patrimonio appare non scevra di problemi, e comunque condizionata dalla casualità delle singole situazioni concrete: rispetto alle vigenti fattispecie di appropriazione (furto, appropriazione indebita) manca (solitamente) lo stesso oggetto materiale tipico della condotta, la « cosa mobile », che difficilmente può essere ravvisato — senza violare il divieto di analogia — ad es. nel denaro « di giro », su cui cade per lo più l'azione di « sottrazione » e di « impossessamento » eseguita operando sui sistemi elettronici di trasferimento dei fondi (EFT). Rispetto alla fattispecie di truffa, poi, come meglio si dirà anche a proposito della sostitu-

Infine, si è rilevato che, se le medesime aggressioni dovessero essere poste in essere nei confronti di sistemi finanziari o di gestione di imprese, enti, ecc, che *non* utilizzano il mezzo elettronico, si « tradurrebbero » per lo più in altrettanti reati di falso, in analoga funzione strumentale rispetto al perseguimento dell'indebito arricchimento o comunque degli scopi illeciti dell'autore.

L'*autonomo* significato sociale di disvalore che tali « mezzi » falsificatori di per sé presentano, non dovrebbe quindi venir meno per il fatto che essi sfruttano la tecnologia elettronica: la loro potenzialità aggressiva e pericolosità sociale, sia sotto il profilo dell'entità del danno cagionabile che sotto quello delle difficoltà di accertamento, appaiono qui anzi ben maggiori[40]. Ed in effetti in certi casi pare preminente, o comunque meritevole di specifica sanzione proprio l'attentato alle aspettative sociali di « genuinità » e « veridicità » dei processi di elaborazione elettronica, soprattutto se gestiscono servizi informatizzati direttamente accessibili al pubblico degli utenti od incidenti sulle posizioni di terzi « estranei ».

Senonché, gravi difficoltà, non solo letterali, si frappongono *de jure condito* a considerare i dati, i programmi ed i risultati di un processo di elaborazione elettronica quali oggetto diretto di protezione penale, ai sensi delle norme di cui al titolo VII cod. pen.[41].

b) Muovendo dall'analisi delle fattispecie disciplinanti le « falsità in atti », occorre subito rilevare che il nostro ordinamento pone ad *oggetto materiale* delle condotte di « falso documentale » solo gli « atti », i « certificati », le « autorizzazioni », le « registrazioni », le « notificazioni », le « scritture », ecc.: tutti termini che, secondo la tradizione interpretativa della dottrina e della giurisprudenza, richiedono innanzitutto la utilizzazione della « forma scritta » (pur intesa in senso lato), quale elemento essenziale di individuazione[42].

Appare perciò estremamente problematico, già sotto questo primo profilo, senza violare il divieto di interpretazione analogica della norma incriminatrice, considerare come documento espresso in forma

zione di persona (art. 494 cod. pen.), non viene integrato di norma l'essenziale requisito modale della « induzione in errore » del soggetto passivo, causa della successiva disposizione patrimoniale a favore dell'agente.

Sul punto si veda ampiamente la dottrina tedesca già sopra citata, cui si aggiungano in particolare, nella letteratura svizzera, STRATENWERTH, *Computerbetrug*, in *Schweiz. Zeit. für Strafrecht*, 1981 (98), 229 s.; RÖHNER, *ComputerKriminalität - Strafrechtliche Probleme bei « Zeitdiebstahl » und Manipulationen*, Zürich, 1976.

Nella dottrina italiana si veda, per veloci spunti problematici, SARZANA, *Note*, cit. (1), 28-29; e, per non convincenti conclusioni, favorevoli alla applicabilità del furto e/o del danneggiamento in tali ipotesi, TRIA, cit. (1), 288 s.

[40] Cfr. sopra, nota (5).

[41] Che « l'alterazione e la cancellazione di dati contenuti nella memoria dell'elaboratore » « molto difficilmente » possa ricadere sotto le previsioni della legge penale italiana relativa al falso, poiché « i dati e le informazioni contenute nel *computer* non possono definirsi giuridicamente "documenti" almeno ai fini della legge penale », viene di recente sostenuto da SARZANA, *Note*, cit. (1), 28-29.

[42] Cfr. per tutti DE MARSICO, *Falsità in atti*, in *Enc. dir.*, XVI, Giuffrè, 1967, 571; CRISTIANI, *Falsità in atti*, in *Noviss. Dig. it.*, VII, Torino, 1957, 5. In giurisprudenza, di recente, Cass. 3 giugno 1977, in *Arch. pen.*, 1979, II, 192, cit. da NAPPI, cit. (30), 643.

scritta, o perlomeno « leggibile da un uomo », l'informazione o l'insieme di informazioni destinate al (od oggetto del) processo di elaborazione elettronica: i « dati informatici » sono costituiti infatti da un complesso coordinato di impulsi magnetici (*bit*), o di altri segni (perforazioni di schede), negativi e positivi, variamente collegati e collocati, funzionali *in modo esclusivo* ad essere « letti » dalla macchina stessa. Ed è evidente che le specifiche « manipolazioni informatiche » che interessa considerare autonomamente sono proprio quelle che intervengono nelle fasi tipiche del processo di elaborazione, in cui le « informazioni » sono espresse in questa forma elettronica o comunque meccanizzata.

Non è però solo la forma (il genere di « linguaggio » utilizzato), perché a ben vedere è lo stesso contenuto, che normalmente rappresenta l'altro elemento essenziale del concetto di « documento » inteso in senso stretto come « atto » o « scrittura », quale oggetto materiale tipico del falso documentale, a essere posto in discussione nel caso di « informazioni » memorizzate elettronicamente o in altro modo meccanico.

Mentre un « documento » è infatti l'« incorporazione » di dichiarazioni o manifestazioni del pensiero *di un uomo*, incorporazione strumentale alla loro *comunicazione* ad un altro soggetto, tanto che ne è elemento imprescindibile, come terzo requisito, la riconoscibilità della *provenienza da un autore* determinato[43], nel caso di dati « informatici » ci si trova molto spesso in presenza di « codificazioni » solo tecniche, espresse in linguaggio macchina, destinate alla comunicazione « interna » con un'altra macchina o con un successivo elemento o momento di elaborazione dello stesso o di altri sistemi automatizzati.

Oltre a non essere visualmente leggibili, tali dati possono non avere cioè neppure alcuna destinazione a costituire *di per sé* « oggetto » di comunicazione né tantomeno « mezzo probatorio » di una dichiarazione di scienza o manifestazione di volontà, proveniente dal pensiero di un uomo, nell'ambito del traffico giuridico, mantenendo invece una funzione esclusivamente « interna » al processo di elaborazione automatica dei dati: ciò avviene in particolare nelle ipotesi (più importanti) di manipolazioni del programma, che pur potendo portare poi ad un risultato *finale* dell'elaborazione « falsificato », non toccano mai l'autenticità e la veridicità dei dati immessi « a monte » né sono « parte » *di per sé*, delle « dichiarazioni » o espressioni risultanti dal processo di elaborazione (*output*), destinate, a valle, ad essere effettivamente comunicate ad altre persone od a ricevere comunque valore probatorio nel traffico giuridico[43-bis].

[43] Sul punto si veda sinteticamente ancora NAPPI, cit. (30), 643-645, con aggiornati richiami di dottrina e giurisprudenza.

[43-bis] Per una dimostrazione convincente del fatto che le manipolazioni di *input* e di programma sfuggono alla previsione delle norme penali sulle falsità documentali (§ 267 StGB), potendo solo quelle di *consol* e manuali, relative alla fase di emissione, essere considerate punibili ai sensi della speciale

Il programma, infatti, è soltanto un insieme di « istruzioni di lavoro » destinato all'*elaboratore*, che prescrive quali operazioni, e con quale sequenza, devono compiersi[44]. Le « manipolazioni » del programma consistono nella soppressione, totale o parziale, di istruzioni « genuine » o/e nella creazione di istruzioni « contraffatte » o « false », che peraltro sono pur sempre destinate *solo* all'elaboratore ed al processo di elaborazione, restando *di per sé* prive di ogni valore « documentale ».

Vero è che il mero fatto della soppressione o cancellazione « abusiva » di istruzioni (o più genericamente di dati) da un supporto magnetico viene da taluno considerata già come danneggiamento, ai sensi dell'art. 635 cod. pen.[45]. In senso contrario occorre però rilevare che non è tanto l'utilizzabilità della « cosa » (pur non considerata nella sua mera sostanza materiale, bensì secondo la sua normale destinazione) ad essere danneggiata o distrutta, perché è soltanto e proprio l'informazione o l'istruzione che essa porta, quale autonomo bene di natura prettamente *immateriale*, ad esserne « cancellata »[46].

In altri termini, ciò che manca è precisamente l'« incorporazione » fra rappresentazione e « supporto », costitutiva invece dell'atto documentale tanto che una volta operata la manipolazione, dell'*input*

norma (priva peraltro di corrispondenza nel nostro ordinamento) del § 268 StGB, che punisce le « falsificazioni » in « riproduzioni meccaniche » automatizzate, cfr. LAMPE, cit. (6), 12 e 18. Conformemente anche SIEBER, cit. (3), 189, ss.); più problematicamente LENCKNER, cit. (1), 33-34, che peraltro non si occupa direttamente del problema.

[44] Cfr. già VON ZUR MÜHLEN, SCHOLTEN, *Computer- Manipolationen aus strafrechtlicher Sicht*, in *NJW*, 1971, 1643, cui si richiama anche LAMPE, cit. (6), 15.

[45] Nella dottrina italiana si veda TRIA, cit. (1), 288, che comunque sottolinea l'opportunità di una più specifica previsione normativa (289); in giurisprudenza, la non convincente, ma interessante, pronuncia del Giudice istruttore del Trib. Torino 12 dicembre 1983, Basile ed altro, in *Giur. merito*, 1984, 1173, nonché in *Giur. it.*, 1984, II, 352 (con nota di FIGONE, *Sulla tutela penale del « software »*) che ha escluso l'ipotesi del danneggiamento (per mancanza di dolo sul requisito dell'altruità della cosa) nella cancellazione parziale di un programma, dato in uso ad una società, da parte di un tecnico della ditta produttrice del *software*. Tale sentenza ha ritenuto però sussistente il reato di esercizio arbitario delle proprie ragioni (art. 392 cod. pen.) ed in specie l'elemento materiale della « violenza » sulla « cosa », ravvisata nella modificazione del suo stato fisico per il « nuovo orientamento dei magnetini che ricoprono la sua superficie » (si badi: del supporto, non certo del programma!) e « soprattutto » nel « mutamento di destinazione rilevabile in relazione all'intero programma di contabilità », che dopo la « mutilazione » non risultava più aggiornabile secondo le successive modifiche economiche e legislative (*ivi*, 357-358).

Tralasciando, per la sua contraddittorietà, la prima argomentazione, ci pare che anche la seconda colga solo la *ratio sostanziale* che rende *meritevole* di previsione penale la condotta considerata, andando però poi oltre i limiti dell'interpretazione (pur estensiva) della norma: l'elemento « violenza sulla cosa » è individuato solo « valutativamente », nel « significato » economico e sociale del risultato finale cagionato, anziché in una precisa *modalità di condotta* tipizzata, avente uno *specifico* oggetto materiale, che non poteva essere costituito dall'*intero* sistema di contabilità, bensì eventualmente solo da una parte *determinata* del suo programma.

Nell'ordinamento tedesco, la maggior parte degli autori e della giurisprudenza ritiene applicabile il reato di danneggiamento (§ 303 StGB) alla semplice cancellazione di registrazioni su nastri (o in genere supporti) magnetici: cfr. per tutti TIEDEMANN, cit. (1), 622 e SCHÖNKE, SCHRÖDER, *Strafgesetzbuch - Kommentar*, Munchen (21ª ed.), 1982, § 303, n. 8).

In senso critico si vedano però i convincenti rilievi di Lampe, di cui alla nota seguente.

[46] Così sostanzialmente LAMPE, cit. (6), 16, con convincente argomentazione.

come del programma, analoga appare la conclusione: il *risultato* dell'elaborazione non potrà « materialmente » essere definito « non genuino » o « contraffatto » o « alterato », rispetto alle modalità di funzionamento dell'elaboratore ed in specifico al parametro offerto dal suo (« nuovo ») *input* o dal suo (« nuovo ») programma, cui fedelmente si attiene[47].

Solo se e quando il *prodotto* finale dell'elaborazione del « linguaggio macchina » verrà riprodotto quantomeno in linguaggio leggibile dall'uomo, e nella misura in cui esso venga o debba venire o si debba presumere destinato alla circolazione giuridica e controllata da un uomo, e da esso, per così dire, fatto proprio, mediante sottoscrizione od in un altro modo inequivoco (come ad esempio nelle forme, attualmente regolate con specifiche norme, degli estratti conto delle banche) potrà nei singoli casi parlarsi nuovamente di « documento » in senso stretto, anche come « atto » o « scrittura » ai sensi del nostro codice penale. E quindi eventualmente anche di una sua mancanza di « genuinità » o « veridicità », rispetto quantomeno ai *presupposti di esso (input* e programma) « pensati » dal suo autore *apparente*.

Ma in tale fase finale la falsificazione sarebbe *già* « esaurita », in contrasto con la ragione giustificatrice dell'incriminazione autonoma dei reati di falso, diretta ad *anticipare* il momento della « consumazione formale » rispetto a quello dell'esaurimento o « consumazione materiale » dell'azione del reo[48].

Infatti il risultato della « falsificazione » potrebbe *già* essere stato utilizzato, in tempo reale, da altri elementi o momenti del processo di elaborazione ed aver prodotto così i suoi effetti dannosi, anche per i terzi: si pensi ad esempio al « blocco » od invece alla possibilità di « illegittima » movimentazione di conti gestiti elettronicamente, od al « parcheggio » abusivo di fondi su conti di terzi, ecc.

La tutela penale offerta dalle attuali fattispecie di « falsità in atti » non solo interverrebbe in un momento troppo tardivo, ma soprattutto sarebbe solo *eventuale*: perché non sempre né necessariamente il risultato della elaborazione è destinato a tradursi (in tempo reale) in una « scrittura » indirizzata all'esterno, potendo questa molto spesso essere finalizzata *solo* ad un immagazzinamento ulteriore o ad una trasmissione ad altre parti o fasi del sistema di gestione automatizzato, non senza peraltro autonomi ed anche rilevanti effetti economici e

[47] È sulla base di analoghe considerazioni che la dottrina tedesca ha concluso per la scarsa operatività ed utilità pratica, in tale campo, della norma pur recentemente introdotta nel codice penale tedesco, di « falso in codici tecnici » (o forse meglio traducibile, in analogia con la locuzione che compare all'art. 2712 del nostro cod. civ., come « falso in riproduzioni meccaniche »), di cui al § 268 StGB, come sostituito dalla prima legge di riforma del diritto penale del 25 giugno 1969 (1 StGB).

Sul punto e sulle innumerevoli (ma anche feconde) polemiche cui ha dato adito l'« infelice » formulazione normativa, si vedano PUPPE, *Vorn Wesen der technischen Auszeichnung*, *MDR*, 1973, 460 (463 e 466); LAMPE, cit. (6), 16; TIEDEMANN, cit. (1), 625; ed *infra*, al par. 5.

[48] Su tale caratteristica dei reati di falso, che ne determinano per molti aspetti la natura « formale », si veda MALINVERNI, cit. (27), 2; CRISTIANI, cit. (27), 172.

« giuridici » nel traffico « informatizzato », che dovrebbe pertanto anch'esso venir equiparato, a certe condizioni, al « traffico giuridico ».

Irrisolto può rimanere, infine, anche il problema della « riconoscibilità » dell'*autore* dell'*output*, e quindi della tutela della provenienza ed *autenticità* del prodotto della elaborazione.

Nel « caricamento » dell'elaboratore operano infatti, ed in tempi diversi, più persone, dal programmatore, all'operatore, al compilatore dei dati, al tecnico addetto alle manutenzioni, ecc.: e molto spesso i loro interventi si risolvono in istruzioni, o modifiche di istruzioni, destinate alla macchina, per cui solo parzialmente, o figurativamente, potrà dirsi che essi sono stati « autori » del contenuto finale dell'*output*.

La provenienza da singole persone identificabili, che intervengono nella memorizzazione ed elaborazione del prodotto finale, può così non venire di regola accertata né « documentata » dall'elaborazione elettronica, che del resto non è finalizzata a tale scopo. Conseguentemente, non potrebbe neppure dirsi « non autentico », per la sola eventuale sostituzione *fraudolenta* di un operatore ad un altro, il risultato dell'elaborazione stessa.

Ciò vale soprattutto nella fase della « circolazione interna » dell'*output* nella singola azienda, ente od amministrazione, che può peraltro essere assai ampia e rilevante; mentre, nei rapporti « esterni », « autore » dell'elaborato « informatico » dovrebbe pur sempre essere considerata la ditta o l'autorità da cui proviene o per conto della quale è prodotto l'*output*[49], in analogia con la pacifica esclusione della qualità di autore del semplice compilatore materiale di un documento[50].

Le ragioni delle difficoltà, qui solo velocemente indicate, a ricondurre le manipolazioni informatiche alle falsità in « atti », ci pare siano riconducibili in definitiva alla stessa essenza delle attività del *computer*, le quali, nonostante vengano « programmate » dal pensiero umano, non sono certo in quanto tali né assimilabili a questo pensiero, né riducibili, nelle loro diverse fasi, con precisa e meccanica corrispondenza, a quelle eseguibili da un mero « strumento operativo » o di espressione del primo (ad es. come si può dire di una macchina per scrivere).

L'aiuto specifico dell'elaboratore elettronico non è infatti tanto o solo quello di « esprimere », sia pur tecnicamente, un certo risultato finale, già concepito dall'autore ed a lui interamente riferibile come *sua* dichiarazione di volontà o di scienza.

L'attività dell'elaboratore consiste invece precisamente nell'*elaborare*, nel *produrre* detto risultato finale, muovendo da certi dati di partenza e secondo un programma predisposto.

[49] Per tale conclusione cfr. SIEBER, cit. (3), 33-34.

[50] In tal senso cfr. per tutti NAPPI, cit. (30), 644.

In definitiva, il risultato finale si può dire « pensato » dall'uomo solo nei suoi presupposti, che sono l'*input* e il programma, cioè solo *potenzialmente*, mentre nella sua effettività è il *computer* che lo produce, dato che la specifica attività di « elaborazione automatica » consiste appunto nello svolgere un'attività che il cervello di un uomo non avrebbe potuto eseguire effettivamente o comunque non ha eseguito nel medesimo tempo, in quelle condizioni[51]. La specifica e sia pur relativa « autonomia » dell'elaborazione automatizzata rispetto alla attività di pensiero dell'uomo non può così non riflettersi nello stesso inquadramento giuridico di condotte che vi incidano « dall'interno », vale a dire « sfruttando » le medesime regole tecniche di produzione e sviluppo di dette « attività », e quindi la sempre possibile « ulteriore » circolazione, connessione, e comunicazione *automatica* di dati (anche di *output* « intermedi »), che costituisce l'essenza stessa del concetto di elaborazione informatica.

Se quindi, per la casualità di singole ipotesi concrete, può talora ricondursi anche alle comuni fattispecie di falso « documentale » una parte fors'ancora consistente delle « falsificazioni » operate su dati o procedimenti informatici, attraverso la valutazione degli *effetti* poi incidenti sul risultato finale, destinato alla circolazione « esterna » e per questo « fatto proprio » da un soggetto che comparirà come suo autore, non di meno ci pare resti evidente l'attuale inadeguatezza delle norme del nostro codice (come del resto dei codici penali di molti altri paesi industrializzati)[52] a riabbracciare specificatamente tali « nuove » condotte illegittime e soprattutto a coglierne l'intimo ed « autonomo » nucleo di disvalore.

Se la *mera* formazione di dati elettronici falsi, od alterazione di dati elettronici veri, nonché la loro *immissione* in un elaboratore elettronico, come pure la semplice « manipolazione » di un programma, *di per sé* considerata, non può oggi ricondursi ad alcuna delle fattispecie penali di falso documentale previste nel nostro ordinamento, ne consegue che anche le condotte preparatorie e successive alla « falsificazione », ed in specie l'*uso* di per sé considerato[53], del dato elettronico falso (il c.d. falso improprio), resta penalmente irrilevante, ai sensi delle norme che rafforzano la tutela della veridicità ed autenticità dei documenti (si pensi in specie all'art. 489 cod. pen.); salvo, ovviamente, che non integri un altro reato (contro il patrimonio, ad esempio), la cui integrazione peraltro, come s'è detto, non è sempre agevole affermare.

Così come la semplice « cancellazione » di dati « veri » o di (una parte di) un programma, pur contenente istruzioni « autentiche »,

[51] Cfr. per tali rilievi già LAMPE, cit. (6), 7, in polemica con la contraria posizione sostenuta invece da KIENAPFEL, *Urkunden und technische Aufzeichnungen*, in *JZ*, 1971, 163.

[52] In tal senso si veda da ultimo SIEBER, cit. (3), 18-20, che dà un quadro anche delle iniziative di riforma intraprese in Stati esteri diversi dalla Germania occidentale.

[53] Sempre che non integri gli estremi di altri reati, ad es. contro il patrimonio.

non potrebbe già di per sé integrare il reato di cui all'attuale art. 490 cod. pen. (soppressione, distruzione e occultamento di atti veri)[54].

c) La minuziosa *descrittività* dell'elencazione degli altri oggetti di tutela considerati nel titolo VII, capi I e II, del libro II del codice penale sulla fede pubblica, non pare consenta di ravvisare altre disposizioni in grado di colmare le cennate lacune: né le norme poste a tutela della moneta (art. 453 ss. cod. pen.), né quelle relative alle carte di pubblico credito ed equiparate (art. 458 cod. pen.), cui non potrebbe assimilarsi, ad es., neppure la carta « Bancomat », né quelle sui sigilli od altri « contrassegni », che pure potrebbero rappresentare, *de jure condendo* e seguendo una diversa tecnica normativa, un settore di riferimento per la previsione di falsità « non documentali » (in senso stretto).

Una considerazione particolare potrebbero avere invece le fattispecie di « falsità personale », di cui al capo IV, per colpire quelle manipolazioni o quegli interventi « strumentali », relativi alla « identificazione » ed « autenticazione » dell'identità dell'operatore[55], necessari per ottenere un accesso « abusivo » all'elaborazione. Senonché, *de jure condito*, la norma generale che punisce la « sostituzione di persona » (art. 494 cod. pen.) non sembra poter soccorrere, poiché la tutela penale vigente richiede come elemento essenziale, vero e proprio evento consumativo del reato[56], l'« induzione di *taluno* in errore ».

Viceversa, nelle « frodi » al *computer* (si pensi al caso italiano già citato delle « truffe » agli sportelli Bancomat) non può mai parlarsi di un « errore » dell'elaboratore nell'identificazione dell'operatore. E se anche esso si ritenesse configurabile, in astratto, rispetto a quelli che erano gli scopi della programmazione di certe misure di sicurezza e controllo, non integrerebbe però mai la realtà psicologica corrispondente a quella della definizione legale, che si riferisce espressamente all'errore cagionato nel processo decisionale di una *persona* umana. Questo potrebbe sussistere solo se, casualmente, a monte o a valle, venisse in rilievo *anche* un errore da parte del titolare del potere di vigilanza sull'elaboratore o meglio del suo rappresentante destinato ai controlli, che non avvedendosi della manipolazione o sostituzione non bloccasse, ad. es., il *computer*. Ma difficilmente tale errore potrebbe considerarsi l'evento perseguito con la condotta di manipolazione dell'agente, e quindi oggetto del suo dolo: la « manipolazione » dei dati di riconoscimento o comunque la « sostituzione di persona » nel momento della identificazione dell'operatore da parte dell'elaboratore viene posta in essere infatti (e finalizzata anche soggetti-

[54] Per ciò che concerne la possibilità, da noi criticata, di applicare in tali casi la fattispecie di danneggiamento, si veda sopra, nota (45).

[55] Cfr. *supra*, par. 2, in fine.

[56] La dottrina italiana è pacifica al riguardo: cfr. per tutti CATELANI, *I delitti di falso*, Milano, 1978, 260; CRISTIANI, *Falsità personale*, in *Noviss. Dig. it.*, VII, Torino, 1968, 24 (25).

vamente) non già per eludere il controllo *successivo* ed eventuale dell'uomo, bensì per consentire direttamente di azionare le operazioni automatiche del *computer*, per provocarne in tempi reali una « decisione » operativa di un certo tipo (l'autorizzazione all'accesso, la consegna del denaro, ecc.).

Tanto che, se controllata dall'uomo, la « falsificazione » difficilmente sarebbe idonea a indurlo in errore e comunque, anche ove ve lo inducesse, tale « errore » non corrisponderebbe all'evento voluto dall'agente[57].

La peculiare autonomia dei processi di elaborazione elettronica dei dati, infatti, come sopra abbiamo già sottolineato, consiste proprio nella diretta ed automatica esecuzione, in tempo reale, di attività « decisionali », quali (nell'esempio degli sportelli Bancomat) quella di una « disposizione patrimoniale », consistente nella consegna della quantità di denaro richiesto, a chi si presenta allo sportello immettendo determinati dati di identificazione.

In tal modo, l'eliminazione della possibilità della « induzione in errore » di un soggetto umano discende già logicamente dall'utilizzo stesso dello strumento tecnologico, finalizzato per l'appunto ad eliminare o meglio sostituire l'intervento diretto dell'uomo in tutta la fase « programmata ».

Esclusa l'applicabilità dell'ipotesi generale di cui all'art. 494 cod. pen., l'unica norma che potrebbe mantenere un proprio spazio di operatività anche nell'ambito di sistemi informatici, data la sua « genericità » nella descrizione dei requisiti modali della condotta (« compensata » dalla perfino eccessiva specificità nell'indicazione dell'oggetto di tutela), ci pare quella di cui all'art. 497 cod. pen., che punisce « chiunque si procura con frode un certificato del casellario giudiziario ». Il semplice termine « frode » può infatti lasciare spazio alla sussunzione di condotte « manipolatorie » realizzate anche direttamente nei confronti del sistema automatizzato di rilascio dei certificati (come già detto introdotto in Italia in numerosi uffici)[58], senza che si richieda — come avviene invece per la truffa o la sostituzione di persone — l'induzione in « errore » di una *persona*. Ad analoghe argomentazioni del resto si è richiamata la giurisprudenza francese, che facendo leva sulla « indeterminatezza » della locuzione *manoeuvre fraudauleuse* su cui si impernia la comune fattispecie di truffa in quell'ordinamento, applica senza difficoltà tale norma anche alle ipotesi realizzate a danno di sistemi informatici[59].

[57] Argomentazioni analoghe sono sviluppate dalla dottrina di lingua tedesca per dimostrare la inapplicabilità, normalmente, della comune fattispecie di truffa (§ 263 StGB) alle « frodi informatiche ».

Sul punto si veda da ultimo TIEDEMANN, cit. (1), 624. Più dettagliatamente, fra i molti, LENCKNER, cit. (1), 25-28, SIEBER, cit. (5); STRATENWERTN, cit. (39), 230-231.

[58] Cfr. in specie GIANNANTONIO, cit. (2), 126 ss. Sull'art. 497 cod. pen. in genere, quale « falsità personale impropria » in cui le « modalità pratiche e particolari » della frode non hanno rilevanza, cfr. CRISTIANI, cit. (56), 27.

[59] Così TIEDEMANN, cit. (1), 629.

5. Può essere significativo, in sede di conclusioni, vista la ricchezza del dibattito che sta accompagnando nella Repubblica federale di Germania non solo la ricerca teorica dei penalisti, ma anche l'iniziativa del legislatore su tali temi, un cenno comparativo sulle soluzioni normative proposte per colmare le lacune riscontrate nella legislazione vigente, per diversi profili assai vicina alla nostra.

La prevalente dottrina tedesca è giunta a ritenere inapplicabili, nella maggior parte dei casi di manipolazioni informatiche, le comuni fattispecie di falsità documentale (§ 267 StGB) e di falsità in codici tecnici (§ 268 StGB) previste attualmente dal codice.

Il fatto che i dati memorizzati elettronicamente o meccanicamente non siano visualmente leggibili o comunque comprensibili dall'uomo, non consistano in una sua dichiarazione di volontà o di scienza, né consentano facilmente di riconoscerne l'autore, e molto spesso non siano neppure destinati ad una funzione probatoria nella circolazione giuridica esterna, comporta che agli stessi non possa essere riconosciuta la qualifica di « atto documentale » (*Urkunde*) che costituisce l'oggetto materiale della condotta descritta nel § 267.

Neppure la nuova e discussa fattispecie di « falso in codici tecnici », introdotta con la legge di riforma del 1969 (attuale § 268 StGB) pare del resto soccorrere adeguatamente. Questa fattispecie tutela infatti l'integrità delle « *rappresentazioni* di dati, di valori di calcolo o di misura, di condizioni o processi reali, prodotte in tutto o in parte automaticamente da un apparecchio tecnico ». La norma fa cioè riferimento specifico a procedimenti di *rappresentazione* automatica, ottenibili con macchine fotografiche, registratori, tachigrafi, bilance automatiche, elettrocardiografi, ecc., vale a dire con strumenti tecnologici moderni, anche « elettronici », che si limitano però ad una « riproduzione » in segni tecnici, ad una « perpetuazione », come si afferma in dottrina[60], di fatti o dati esistenti nella realtà fenomenica e dunque non « prodotti » dall'elaboratore stesso. Pur distinguendosi perciò dai « documenti » in senso stretto, perché non richiedono a proprio contenuto una « dichiarazione di pensiero » di un uomo, né un « autore » riconoscibile, essi non riabbracciano l'essenza « dinamica » dei dati e risultati del processo non meramente riproduttivo, ma anche in parte « decisionale » ed « innovativo », proprio nell'elaborazione elettronica.

Neppure il comma 3 della nuova norma, che estende il concetto di « falsificazione del codice tecnico » anche alle ipotesi in cui l'« agente influisca, con intervento disturbatore del procedimento di codificazione, sul segno tecnico risultante » appare coprire il campo delle manipolazioni informatiche: esso infatti potrà trovare applicazione solo nelle « marginali » ipotesi di manipolazioni cosiddette di *consolle*, poste in essere intervenendo materialmente, a procedimento di « elaborazione » concluso o interrotto, sulla sola *espressione* (o, ap-

[60] Sul punto si veda, peraltro criticamente, PUPPE, cit. (47), 461.

punto, « riproduzione ») dei *risultati* dell'elaborazione stessa[61]. Mentre non potrà trovare applicazioni nelle più frequenti e significative manipolazioni della elaborazione in quanto tale, irriducibile ad un mero processo di riproduzione tecnica, in un certo codice, dei dati di partenza.

Per tali ragioni, accogliendo istanze avanzate da tempo in dottrina, è stata proposta la nuova autonoma fattispecie di « falso in dati memorizzati », inserita dal Governo federale nel progetto di « Seconda legge per la lotta alla criminalità economica » (2 WKG), presentato fin dal 1982 al Parlamento tedesco[62].

Secondo il testo di tale norma, costituisce reato il fatto di chi « al fine di inganno nei rapporti giuridici, modifichi dati senza autorizzazione, ovvero faccia uso di dati modificati senza autorizzazione, i quali, invisibili o immediatamente leggibili (dall'uomo, *N.d.t.*), siano stati memorizzati elettronicamente, magneticamente od in altro modo, e siano destinati, attraverso l'elaborazione, ad essere utilizzati nei rapporti giuridici, come elementi probatori di fatti giuridicamente rilevanti ». La pena prevista è identica a quella dei « comuni » reati di falso documentale e falso in codici tecnici, di cui ai citati §§ 267 e 268 StGB (pena detentiva fino a 5 anni o pena pecuniaria).

Innanzitutto va segnalata la scelta consapevole di prevedere una nuova ed autonoma incriminazione per tali fatti, anziché limitarsi ad ampliare semplicemente la comune fattispecie di falso documentale.

Sul piano sistematico ciò evidenzia la sostanziale individuazione di un nuovo « bene » oggetto di tutela; mentre sul piano tecnico-interpretativo evita l'estensione, ad un elemento del tutto eterogeneo (come il concetto di « dato elettronico »), del tradizionale concetto di « documento », che avrebbe potuto portare a grosse difficoltà applicative.

Del resto, l'ampiezza ed il significato economico-sociale, nel traffico giuridico della società contemporanea, della gestione automatizzata dei « dati » giustifica ampiamente la previsione di una nuova autonoma fattispecie, che richiami anche l'attenzione della opinione pubblica e degli operatori giuridici sulla rilevanza di tali condotte delittuose.

Molto discusso è però ancora l'ambito che deve avere tale tutela penale: si è rilevato infatti che essa non deve né può garantire la « ve-

[61] Così espressamente LAMPE, cit. (6), 16.

[62] Si tratta di Br-Drucks. 150/83 del 6 aprile 1983, corrispondente al BT-Drucks. 10/318 del 26 agosto 1983, Allegato n. 1, 4 ss., che riproduce, per ciò che concerne le fattispecie sulla criminalità informatica, il precedente disegno governativo BR-Drucks. 219/82 del 4 giugno 1982 ed il progetto, ripresentato nella nuova legislatura dai deputati della SPD, BT-Drucks. 10/119 dell'8 giugno 1983.

Per la traduzioni delle principali norme di tale progetto ed alcuni riferimenti essenziali si veda PICOTTI, cit. (23), 620 s. Per una completa citazione del vasto materiale dei lavori preparatori si rinvia a SIEBER, cit. (3), 43 s., nota (57).

Di grande interesse è in particolare il resoconto della seduta del 6 giugno 1984 della Commissione giuridica del *Bundestag*, in cui hanno preso posizione significativi esponenti della dottrina penalistica (Haft, Sieber, Paul, Mohr, Oertel, Lehnhoff e Brentrup).

rità » oggettiva di *tutti* i dati memorizzati elettronicamente[63]. Lo stesso diritto penale vigente solo in ristretti casi eccezionali tutela del resto la « verità sostanziale » dei « documenti ». La sanzione penale deve piuttosto operare contro gli interventi « non autorizzati » (*unbefugt*) sui sistemi informatici, che pongono in pericolo ed aggrediscono la affidabilità anche « probatoria » dei dati e risultati delle elaborazioni.

Pertanto la norma dovrebbe riabbracciare solo le azioni manipolative di persone « non competenti », cioè estranee all'azienda od all'ente che gestisce l'elaboratore, oppure anche interne ad essi, ma che agiscano al di fuori della loro sfera di « competenze » ed attribuzioni[64].

In tal modo, si potrebbe distinguere la « falsità » di per sé punibile come autonomo titolo di reato, dal più ampio concetto di « intervento scorretto (*unrichtig*) o non autorizzato », comunque influente sui processi di elaborazione, previsto come costitutivo ad es. del nuovo delitto di « truffa mediante *computer* » (§ 163 *a* StGB), pure inserito nel citato progetto di legge. Questa seconda fattispecie, specificamente indirizzata alla tutela del patrimonio, seleziona infatti con altri criteri la sfera della punibilità, richiedendo due ulteriori elementi, tipici della truffa « comune »: la conseguente causazione di un danno patrimoniale altrui e il fine di ingiusto profitto[65].

Altre norme completano infine l'equiparazione del reato di « falso in dati memorizzati » ai comuni reati di falso documentale, coordinandone l'inserimento nel sistema.

[63] Riassuntivamente SIEBER, cit. (3), 45 s.

[64] Sul punto cfr. in specie BUNDESMINISTERIUM DER JUSTIZ (Hrsg), *Tagungsberichte der Sacheverständigen Kommission zur Bekämpfung der WirtschaftsKriminalität*, Vol. 12°, Berlin, 1977, 85.

Vanno qui segnalate anche alcune proposte di modifica e completamento del testo normativo, dirette in particolare ad estendere la previsione penale alla stessa « memorizzazione non autorizzata » (quindi anche « originaria ») di dati, proposta dal *Bundesrat* e recepita in parte dal Governo federale (cfr. BT-Drucks. 10/318 del 26 agosto 1983, Allegato 3, 55-57, riportato in appendice a SIEBER, cit. (3), 73-74); nonché a riabbracciare espressamente anche le manipolazioni, nella fase di *output*, che si limitino ad *impedire* in tutto o in parte la espressione di (determinati) dati. Su queste, come su analoghe proposte che paiono troppo orientate ad una minuziosa casistica, condizionata dalle contingenti caratteristiche dell'attuale livello della tecnologia elettronica, con il rischio poi di una rapida obsolescenza di fronte a nuovi sviluppi dell'informatica, si veda convincentemente SIEBER, cit. (3), 46 s. e, più in generale, 33 s., ove (in polemica con il « perfezionismo » tecnico di LENCKNER, WINKELBAUER, *Strafrechtliche Probleme im modernen Zahlungsverkehr*, in *Wistra*, 1984, 83 s.) auspica una *semplificazione* nella struttura delle nuove fattispecie, che limiti al massimo il ricorso a concetti tecnici e colga piuttosto sinteticamente la concezione strutturale, l'*idea* che sta a fondamento (*Strukturdenken*) dei sistemi informatici e telematici.

Per questo egli propone ad esempio che la stessa formulazione del « nuovo » § 269 StGB (sopra riportata nel testo) venga rivista, prevedendosi la punibilità di « chiunque, a fine di inganno nei rapporti giuridici, *senza autorizzazione ponga in essere immissioni o modificazioni in un sistema di memorizzazione automatica di dati*, che siano destinati a provare circostanze giuridicamente rilevanti, ovvero faccia uso di dati influenzati da tali immissioni o modificazioni non autorizzate » (corsivi nostri).

[65] Su tali esigenze si veda criticamente STRATENWERTH, cit. (39), 232, che pur muove dalla diversa situazione normativa dell'ordinamento svizzero; nonché, di recente, l'esauriente ed esseziale sintesi di SIEBER, cit. (3), 26 s.

In particolare viene considerato « equivalente » all'inganno nel « traffico giuridico » quello nell'« elaborazione dei dati » (§ 270 StGB), mentre la cancellazione o soppressione « abusiva » di dati viene equiparata alla soppressione di documenti (§ 274 StGB)[66].

6. In definitiva, la ricchezza del dibattito in materia e l'ampiezza della casistica ormai nota, ci pare dimostrino l'urgenza e necessità di un approfondimento di tale tematica anche nel nostro paese, per poter preparare e insieme sollecitare tempestivi interventi del legislatore, che evitino pericolose lacune dell'ordinamento e non meno pericolose violazioni del principio di stretta legalità nella prassi penale.

Superfluo è sottolineare d'altronde l'importanza che una regolamentazione normativa chiara e tassativa in tale settore, può fin da subito avere, visto il ruolo determinante che nello sviluppo delle relazioni economiche, politiche e sociali è ormai affidato ai sistemi informatici.

[66] SIEBER, cit. (3), 47, propone però che la descrizione della condotta costitutiva di tale fattispecie non si limiti all'indicazione delle forme finora più note (« cancellare » e « sopprimere » dati), ma si orienti ad una nozione più ampia, come ad esempio quella di « rendere inutilizzabili ».