

GIOVANNA CORRIAS LUCENTE

INFORMATICA E DIRITTO PENALE: ELEMENTI PER UNA COMPARAZIONE CON IL DIRITTO STATUNITENSE (2^a PARTE)

III. TUTELA DEI DATI E DEI PROGRAMMI PER ELABORATORE

1. *Apprensione e danneggiamento dei dati e dei programmi attraverso il loro supporto fisico.*

La più recente legislazione americana, oltre alle ipotesi di accesso abusivo e furto dei servizi di un elaboratore, ha anche preso in considerazione altre manifestazioni della criminalità informatica, segnatamente consistenti nell'abusiva apprensione, danneggiamento od alterazione dei dati o dei programmi per elaboratore.

In proposito l'attenzione sarà concentrata esclusivamente sugli aspetti comuni ad ogni forma di apprensione non autorizzata di programma e dati, rinviando invece ai numerosi studi specifici per l'esame delle altre tipologie di abuso, quali ad esempio la violazione dei diritti d'autore o di privativa¹⁴⁷.

* La prima parte della presente ricerca è stata pubblicata in *Dir. inf.*, 1987, 167.

¹⁴⁷ Cfr. AA.VV., *La tutela del software* a cura di G. ALPA, Milano, 1984; F. MINERVA, *La illiceità penale della riproduzione di programmi altrui: l'orientamento della Cassazione e le prospettive sanzionatorie*, in questa *Rivista*, 1987, 696; R. RISTUCCIA, *Discordanti indirizzi giurisprudenziali in materia di software e videogiochi*, in questa *Rivista*, 1986, p. 168, con attenzione alla giurisprudenza e legislazione nord americana in materia di proteggibilità dei programmi per elaboratore attraverso il *copyright*, ed alle recenti legislazioni francese (legge 3 luglio, 1985, n. 85-660); tedesco occidentale (*Gesetz zur Änderung vor Vorschriften auf dem Gebiet des Urheberrechts* del 24 giugno 1985) (cfr. al riguardo L. PICOTTI, *La nuova normativa*, cit., p. 1); ed inglese (*Copyright Amendment Act* del 16 luglio 1985). Specificamente per gli Stati Uniti cfr.: L. WHARTON, *Use and Expression: the Scope of Copyright Protec-*

tion for Computer Programs, 5 *Computer L.J.*, p. 433, 1985; D.E. STOUT, *La brevettabilità del software nella più recente legislazione americana*, in questa *Rivista*, 1986, p. 69; C. TAPPER, *Computer and the Law*, Harlow, 1983, con riguardo agli orientamenti giurisprudenziali americani ed inglesi (precedenti la novella della legge sul *copyright*); per la Francia v. i commenti alla legge di: A. MANNA, *Aspetti problematici della c.d. criminalità informatica nei paesi francofoni*, in questa *Rivista*, 1987, p. 503; R. PLAISANT, *La loi n. 85-660 du 3 juillet 1986*, in *J.C.P.*, 1986, doc. 3230; M. VIVANT, *Le logiciel au pays des merveilles*, in *J.C.P.*, 1986, doc. 3208; J. HUET, *Les logiciels sont protégés par le droit d'auteur*, D. 1985, Chr. 261. Per un'analisi comparatistica della problematica: U. SIEBER, *The International*, cit., p. 41, che esamina anche *The Forgery and Counterfeiting Act* del 1981, legge inglese applicata anche alle falsificazioni informatiche.

Il problema della tutela dei dati memorizzati o dei programmi per elaboratore, si atteggia in maniera diversa a seconda della modalità prescelta per la loro apprensione o distruzione.

Viene innanzitutto in rilievo il caso in cui l'appropriazione od il danneggiamento abbiano ad oggetto contemporaneamente i dati od i programmi ed il supporto in cui essi trovano incorporati. Si può immediatamente senza difficoltà riscontrare che la qualificazione penale di tali fatti non pone particolari questioni, in quanto negli S.U. (come del resto ovunque) sono previsti dalla preesistente normativa ed integrano reati come furto o danneggiamento che rappresentano delle vere e proprie costanti nei diversi ordinamenti giuridici¹⁴⁸.

Purtuttavia le recenti leggi emanate da alcuni Stati americani contro la criminalità informatica, introducendo il reato di danneggiamento dei dati o di programmi, hanno finito per sanzionare ulteriormente questa condotta, inasprendo le sanzioni che a tali fatti sarebbero state applicabili secondo la maggior parte delle leggi previgenti¹⁴⁹.

2. *L'apprensione del solo contenuto.*

Questioni di ben diverso ordine sorgono invece al momento in cui l'apprensione o la distruzione investano esclusivamente i dati od i programmi nel loro contenuto senza coinvolgere il relativo substrato materiale.

Nonostante la loro intrinseca incorporalità, tali beni hanno acquisito rilevante valore economico: i programmi, in quanto prodotto dell'ingegno suscettivo di sfruttamento e di applicazioni economiche; i dati, considerati singolarmente, per la loro originalità o riservatezza; complessivamente, in ragione del lavoro richiesto per la raccolta e l'organizzazione.

La problematica che si è andata sollevando circa la protezione da conferire ai dati ed ai programmi, in virtù della loro rilevanza patrimoniale, coincide parzialmente con quella insorta per la tutela penale dell'informazione in genere. V'è tuttavia al riguardo da considerare che le possibilità di lesione dei diritti sull'informazione sono aumentate in maniera esponenziale attraverso l'introduzione dei sistemi informatici, che hanno reso più agevole, e comunque più frequente, l'apprensione di beni mediante la loro copia od il danneggiamento dei medesimi (mediante la loro cancellazione totale o parziale) consentendo anche di realizzare tali attività solo attraverso i mezzi elettronici e di prescindere, dunque, dal fisico contatto con i dati. Si può, infatti, ottenerne la copia facendo semplicemente apparire le infor-

¹⁴⁸ Per gli S.U., sulla configurabilità del reato di *mischief* e di *larceny* previsto dalla legislazione statale e Federale: U.S. DEPARTMENT, *op. ult. cit.*, pp. 2, 3, 9.

¹⁴⁹ In generale v. *infra*, par. VI.

mazioni sul videoterminale, ovvero ordinando una riproduzione del contenuto attraverso la stampante di un elaboratore anche a grande distanza dal centro di elaborazione dei dati; e parimenti si può provocare la cancellazione sfruttando l'apposito programma e compiendo la serie di ordini necessari alla sua esecuzione.

Due dati differenziali, dunque, possono ricavarsi rispetto alle condotte altrimenti aggressive di beni immateriali, analoghi ai dati ed ai programmi: la loro concentrazione e la loro accessibilità attraverso i mezzi elettronici, caratteristiche entrambe che comportano una maggiore vulnerabilità¹⁵⁰.

Nonostante tali differenze le soluzioni offerte a livello interpretativo in materia di dati, ripetono, sostanzialmente, il contenuto di quelle già proposte riguardo alle informazioni in generale.

3. Qualificazione del fatto nella legislazione federale comune.

Negli Stati Uniti, in assenza di specifiche previsioni legislative, a livello federale, si è talora cercato di estendere alle attività di copia o comunque di apprensione dei dati o dei programmi, la normativa penale posta a tutela della proprietà¹⁵¹. Si è trattato in sostanza di colmare una lacuna normativa applicando ai dati ed ai programmi, nonostante la loro intangibilità, le norme penali concernenti i beni materiali.

Il tentativo di attribuire una protezione attuale per i dati ed i programmi si è andato estrinsecando in due decisioni giudiziali oltremodo significative. Si tratta del noto caso deciso nelle sentenze U.S. v. *Girard*¹⁵² e U.S. v. *Lambert*¹⁵³: un agente della D.E.A. (*Drug Enforcement Agency*), Girard, valendosi d'un preposto, Lambert, autorizzato all'accesso all'elaboratore dell'ufficio, aveva ottenuto e rivelato, dietro congruo compenso, ad un agente provocatore del medesimo ufficio, i nominativi di altri agenti ed i piani di alcune indagini per colpire il traffico della droga. In entrambi i giudizi la Corte federale ha ritenuto configurabile, nella condotta posta in essere dagli imputati, il reato di *larceny* (una figura comprendente talune condotte tipiche per la realizzazione del furto e dell'appropriazione indebita). Tale esito è stato però agevolato dalla particolare formulazione della norma incriminatrice applicata al

¹⁵⁰ Si v. quanto al valore delle informazioni le considerazioni svolte da M.P. LUCAS DE LEYSSAC, *Il furto d'informazione*, in questa *Rivista*, 1985, p. 625, part. p. 627 ss.

¹⁵¹ In genere, su tale impostazione v. A. ALESSANDRI, *op. cit.*, p. 48 ss.; E.A. GLYNN,

op. cit., p. 78, 82; WHITE COLLAR CRIME, *A survey*, cit., p. 374; U. SIEBER, *The International*, cit., p. 55.

¹⁵² U.S. v. GIRARD, 601 F2d, 69 (2nd Cir. 1980).

¹⁵³ U.S. v. LAMBERT, 446 F. Supp., 890 (D. Conn. 1978).

caso: il *larceny*¹⁵⁴, infatti, 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, realizzata dagli imputati, in secondo luogo in quanto contempla quali oggetti del reato, oltre alle « cose di valore » anche i *records* (cioè qualsiasi informazione trascritta).

La Corte federale ha perciò potuto ritenere che nella nozione di « cose di valore » vadano ricomprese anche le copie delle informazioni economicamente rilevanti, considerando che le informazioni medesime sono già parzialmente tutelate attraverso il riferimento al termine *records*, valido a designare anche il contenuto dei documenti originali¹⁵⁵.

Le due pronunce si fondano entrambe sul richiamo di un'interessante serie di precedenti giurisprudenziali, relativi all'apprensione di informazioni non memorizzate nell'elaboratore¹⁵⁶, le quali tuttavia non appaiono raggiungere in maniera così diretta le conclusioni invece accolte dalla Corte nel caso dianzi descritto¹⁵⁷.

L'orientamento interpretativo espresso nelle sentenze U.S. v. Girard e Lambert è stato valutato in maniera divergente, talora come manifestazione d'una mutata sensibilità giurisprudenziale rispetto alla tutela dei dati informatici e delle informazioni in genere, talaltra come un'isolata pronuncia insuscettibile di esser secondata in maniera generalizzata, per la quantità e la qualità dei limiti che si frappongono all'applicazione ai dati od alle informazioni delle norme sui beni materiali¹⁵⁸. È, inoltre, opportuno aggiungere che per un contra-

¹⁵⁴ La norma (par. 641) è riportata sopra alla nota 72.

¹⁵⁵ Cfr. U.S. v. LAMBERT, *cit.*, p. 895. La Corte ha, inoltre considerato che la storia legislativa della norma non è determinante in ordine all'applicabilità di essa alle cose intangibili; e che i dati, confidenziali conservano un valore solo finché restano nell'esclusiva disponibilità del governo.

¹⁵⁶ Si tratta delle decisioni (U.S. v. di GILIO, 538 F2d, 972 (3d Cir. 1976): copia periodica di documenti del FBI e vendita al soggetto interessato alle indagini; U.S. v. FRIEDMAN, 445 F2d, 1076, (9th Cir.) copia e vendita di documenti segreti del *Grand Jury* (citati in U.S. v. LAMBERT); U.S. v. BOTTONE, 365 F2d, 389 (2d Cir.) condannato per « trasporto illecito di merci », consistenti in colture di microrganismi. In U.S. v. GIRARD si riportano, inoltre, precedenti che non concernono il reato previsto dal par. 641, ma concorrono a dimostrare che anche i beni intangibili sono circondati di tutela penale, con riguardo: ai divertimenti (GIOMI, v. CHASE, 47 N.M., 22 (1942); incontri sessuali (Mc Donald v. STATE, 57, Ala App., 529); promessa d'impiego (People ex rel. Dickinson v. VAN DE CARR, 87, App. div., 386); accordo

per non presentarsi alle elezioni (People v. HOCHBERG, 62, A.D. 2d, 239).

¹⁵⁷ Alcuni casi, infatti, non riguardano propriamente le informazioni. Nel caso U.S. v. di GILIO, *cit.*, l'imputazione di furto non concerneva esclusivamente le informazioni, ma anche la carta che era stata sottratta. In U.S. v. BOTTONE, *cit.*, il trasporto e l'illecita apprensione (presupposto dello specifico reato contestato) riguardavano pur sempre oggetti materiali. L'unico precedente specifico pare perciò esser U.S. v. FRIEDMAN, *cit.*, in cui l'imputato aveva copiato i documenti trascrivendoli su carta di sua proprietà.

¹⁵⁸ Si vedano i commenti alla sentenza di L. MENNELLY, *op. cit.*, p. 577; A. ALESSANDRI, *op. cit.*, p. 52, ss.; G. THACKERAY, *op. cit.*, p. 248; B.J. GEORGE, *op. cit.*, p. 394; J.T. SOMA, *op. cit.*, p. 282 sottolinea che l'applicazione del par. 641 dipende dall'interpretazione del termine « *thing of value* », che sinora non pare uniforme. Altre questioni al riguardo sono sollevate in WHITE COLLAR CRIME, *A survey*, *cit.*, p. 376, ove si segnala la diversa problematica della ricompressione dell'attività di copia, nella « *conversion* » (esercizio dei poteri spettanti al proprietario).

stante orientamento giurisprudenziale di cui si sono avute recenti espressioni¹⁵⁹, il reato di *larceny* è riferibile esclusivamente ai beni materiali, per ragioni di ordine sistematico. Secondo tale interpretazione, infatti, altrimenti estendere la sfera di applicabilità della norma, comporterebbe un'inammissibile negazione delle scelte di politica criminale effettuate dal legislatore federale, il quale ha inteso tutelare in maniera solo frammentaria e non generalizzata le informazioni, come manifestano le diverse norme sulle violazioni dei segreti, con le quali vengono selezionate le classi di informazioni tutelate; vengono sanzionate solo talune modalità di violazione; e talora persino solo taluni autori del fatto¹⁶⁰.

Altro interessante punto di riferimento della giurisprudenza federale in tale materia può essere considerato il reato di *Interstate Transportation of stolen Goods*¹⁶¹ — consistente nel trasporto interstatale od estero di merci od altri beni, provenienti dai delitti tassativamente indicati, e di valore non inferiore ai 5.000 dollari. L'applicazione di tale previsione di reato è stata vagliata con riferimento a due forme di trasferimento delle informazioni. Innanzitutto con riguardo al trasporto materiale di copie illecitamente apprese, in ordine al quale la giurisprudenza in tema di criminalità informatica ha meramente recepito le indicazioni già espresse da alcune risalenti decisioni¹⁶². Secondo esse ai fini della configurabilità del reato è sufficiente che le copie illecitamente apprese siano incorporate in un supporto fisico, senza che sia necessario il trasporto dell'informazione originale; ed inoltre che il requisito del valore, condizionante la punibilità del fatto, sia apprezzabile in relazione al contenuto immateriale della copia¹⁶³. In tal modo si è attribuito un ruolo di determinante rilievo per la qualificazione del fatto all'informazione in sé considerata, anche se il suo substrato materiale conserva una funzione ineliminabile¹⁶⁴.

¹⁵⁹ U.S. v. TRUONG DINH HUNG, 629, F2d, 923 (Court App. 4th Cir., 1980). Il caso d'un funzionario che aveva arbitrariamente rivelato informazioni sulle trattative in corso fra S.U. e Vietnam del Nord. Tale sentenza contiene un'attenta analisi dei precedenti in argomento; della storia legislativa del par. 641; nonché delle forme di tutela accordate a particolari classi di informazioni attraverso i reati di violazione del segreto.

¹⁶⁰ Cfr. U.S. v. TRUONG, *passim*.

¹⁶¹ 18 U.S.C. par. 2314: « *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* ».

¹⁶² Cfr. U.S. v. BOTTONE, *cit.* (trasporto di colture di microrganismi); U.S. v. LESTER,

282, F 2d, 750 (3d Circ. 1960) e U.S. v. SEAGRAVES, 265 F2d, 876 (3d Circ. 1959); trasporto di copie di mappe geofisiche.

¹⁶³ Al riguardo l'acuta analisi della giurisprudenza nordamericana condotta da A. ALESSANDRI, *op. cit.*, p. 50 ss.

¹⁶⁴ Id. riscontra una certa discrepanza fra le motivazioni delle sentenze che si spingono « con arditezza verso l'assottigliamento dei requisiti materialistici del fatto » e il contenuto delle decisioni che si fondano sulla possibilità di far riferimento ad una condotta almeno strumentale di sottrazione e appropriazione di beni materiali. Cfr., in generale, sull'applicabilità dell'ipotesi di reato alle informazioni: U.S. DEPARTMENT, *op. cit.*, p. 12; WHITE COLLAR CRIME, *A survey*, p. 376; G. THACKERAY, *op. cit.*, p. 304.

Attraverso tale procedimento interpretativo è stato spesso sanzionato a titolo del par. 2314 il trasporto di copie di programmi illecitamente apprese, od anche di videocassette pirata¹⁶⁵. Se in tali casi si è potuto applicare un orientamento giurisprudenziale consolidato, non altrettanto è accaduto allorché si è inteso verificare se il trasferimento di informazioni per via elettronica, dall'elaboratore centrale ad un terminale, potesse configurare il reato di Trasporto di merci illecitamente apprese. Poste dinanzi al quesito, le Corti sono sinora pervenute a conclusioni negative: ritenendo che oggetto del trasporto siano gli impulsi elettronici, i quali, in quanto intangibili, non possono esser ricondotti nel novero dell'oggetto materiale del reato in questione¹⁶⁶.

4. La recente legislazione in materia.

Si è invece rilevato che a livello statale si frappongono maggiori difficoltà per ricondurre nell'ambito dei reati posti a tutela della proprietà le fattispecie concrete in questione. Per quanto la varietà delle disposizioni dei singoli Stati in materia non consenta in questa sede che di rilevare indicazioni di massima, si può considerare che la formulazione delle norme incriminatrici sul furto, spesso diversificandosi da quella contenuta nella disposizione federale, rende esplicito ed insuperabile l'ancoramento delle fattispecie penali ai beni materiali¹⁶⁷. Tale imprescindibile collegamento è talora imposto dalla necessità che l'oggetto del reato sia qualificabile come *property*, tradizionalmente ritenuta afferente solo i *tangible articles*¹⁶⁸; talaltra dalla previsione, quale elemento costitutivo del reato, dell'asportazione — come modalità della condotta o del dolo specifico consistente, *nell'intent of permanently deprive*¹⁶⁹ — che non si realizza nel caso di copia dei dati e dei programmi, considerato che gli originali restano nella completa e costante disponibilità del titolare.

¹⁶⁵ Cfr. U.S. v. GOTTESMAN, 724, F2d, 1517 (11th Cir. 1984) trasporto di copie di film pornografici; U.S. v. BELMONT e Jal., 715 F2d, 459 (9th Cir. 1983) traffico di video cassette. Specificamente in tema di trasporto di copie di programmi: U.S. v. DREBIN, 557, F2d, 1316 (9th Cir. 1977), ove si è considerato che la violazione del diritto d'autore sul programma può costituire il presupposto del reato, consistente nell'illecita apprensione, ma *contra*, v. U.S. v. SMITH, 686, F2d, 234 (c. App. 5th Cir. 1982).

¹⁶⁶ WARD v. SUPERIOR COURT, 3 Comp. L. Serv. Rep., 208 (1972); U.S. v. SEIDLITZ, 589, F2d, 152 (4th Cir. 1978); su questa sentenza cfr. L. WHARTON, *op. cit.*, p. 249; L.

MENNELLY, *op. cit.*, p. 564; A. BEQUAI, *op. cit.*, p. 38.

¹⁶⁷ Nella *common law* il reato di *theft* consisteva nel « *felonious taking and carrying away of the personal property of another, without his consent, and with the intention of permanently deprive him* ». Tale formulazione è stata riprodotta in diversi codici statali. Al riguardo si vedano le considerazioni di A. ALESSANDRI, *op. cit.*, p. 58.

¹⁶⁸ V. *supra*, nt. 72.

¹⁶⁹ Così, A.M. WAGNER, *op. cit.*, p. 787; A. BEQUAI, *Computer*, cit., p. 30; G. THACKERAY, *op. cit.*, p. 309; M.D. SCOTT, *op. cit.*, par. 8.4.

Dinanzi alla carenza di tutela emersa nel previgente sistema rispetto ai dati ed ai programmi informatici, alcuni Stati sono ricorsi ad interventi legislativi, espressamente comprendendo nella nozione di *property* i dati ed i programmi indipendentemente dalla loro insistenza su un supporto materiale, così da estendere anche a tali beni le fattispecie di reato contro la proprietà¹⁷⁰, ovvero le ipotesi speciali di reato introdotte con le leggi sulla criminalità informatica¹⁷¹.

Tali indicazioni legislative non sono rimaste scevre da critiche, le quali sottolineano come in tal modo si sia introdotta una forma di tutela per alcune classi di informazioni considerate in base alla forma della loro conservazione ed a prescindere dal loro specifico contenuto, dal loro valore o dalle caratteristiche che presentano. L'iniziativa è stata ritenuta impropria e suscettiva di essere estesa a tutte le categorie di informazioni, ivi comprese quelle notorie, senza che se ne presenti una effettiva giustificazione sul piano della necessità od opportunità di tutela¹⁷².

Più consono alla particolare natura e connotazione del bene è stato perciò ritenuto¹⁷³ l'intervento legislativo effettuato dallo Stato della Florida, per cui i dati, i programmi e le informazioni destinate ad essere memorizzate sono state qualificate come *intellectual property*¹⁷⁴, e sono state introdotte specifiche ipotesi di reato che comprendono le possibili attività aggressive contro tali beni¹⁷⁴. V'è infatti da rilevare

¹⁷⁰ « *Property includes computer programs or data* », Ill., Crim. Code, sec. 15-1; Va. Code par. 18.2-98.1; Tenn. Code Ann. par. 39-3, par. 1403 (h); inoltre Nev. Rev. Stat. par. 28.5-09 (5) per cui: *property includes tangible or intangible property*.

¹⁷¹ « *For the purpose of this section property means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible*, Ariz. Crim. Code, 13-2301 E8; Cal. Pen. Code, par. 502 (a) (7); Colo. Rev. Stat. 18.5.5-101 (8); Mich. Stat. Ann. par. 28.5 29 (3) (1); N.C. Gen. Stat. Ann. par. 14-453 (8); R.I. 11.52.1 (E); Utah Crim. Code, par. 76-6-702 (5); GA Code par. 16-9-92 (7). In tal modo i dati e i programmi vengono a costituire, certamente oggetto del reato di *computer fraud* (per cui v. *infra*, par. IV). Tuttavia L. WHARTON, *op. cit.*, p. 249 ritiene che attraverso tali interventi legislativi non sia consentito estendere l'applicabilità del reato di furto anche ai dati e programmi. Tale conclusione appare interdetta dall'espressa limitazione, alle leggi sulla criminalità informatica, della qualificabilità come *property* dei dati e dei programmi.

Deve comunque rilevarsi che la semplice apprensione dei medesimi, anche se non seguita dalla copia è punita a titolo di accesso abusivo, essendo in tale nozione ricompresa anche l'attività di « rintracciare i dati memorizzati nel computer », come si ebbe a rilevare *supra*, par. II.

Interessante inoltre segnalare le disposizioni di altri Stati che prevedono l'apprensione o la copia dei dati, programmi o della documentazione di supporto come reato autonomo (Wis. Stat. Ann., par. 94370 (2); Del. Code Ann. tit. 11, par. 935 (1); Nev. Rev. Stat. 205.474; R.I. Gen. L., 11-52.4. Altrove, invece, il fatto è punibile solo se sostenuto dall'intento di privare il proprietario (Iowa, Act of May 10, 1984, par. 6).

¹⁷² L. WHARTON, *op. cit.*, p. 249.

¹⁷³ Id., *op. loc. cit.*

¹⁷⁴ Fla. Stat. ann. par. 815.03 (1): « *Intellectual property means data, including programs* ». Ma anche par. 815.03 (8) « *property... includes, but is not limited to ... information including electronically produced data and computer software and programs* » (si da potersi applicare le ipotesi di *computer fraud*).

che, in tal modo, i dati risultano tutelati per la loro natura riservata, sicché le informazioni notorie non possono essere oggetto del reato in questione¹⁷⁵. Va inoltre rimarcato che ove le informazioni, i dati o i programmi appresi costituiscano per il loro contenuto *trade secret* (nel ricorso degli altri presupposti richiesti dalla legge) potrebbe configurarsi il reato di violazione del segreto industriale, introdotto recentemente in alcuni Stati ma estraneo all'ordinamento federale¹⁷⁶.

Un'inversione delle tendenze legislative volte ad estendere indifferenziatamente la tutela dei dati, anche attraverso l'applicazione dei reati contro la proprietà materiale, parrebbe essersi realizzata a seguito dell'emanazione del *Counterfeit Access Device and Computer Fraud Act*, attraverso il quale è stata conferita tutela, seppur particolarmente avanzata, solo a talune classi di dati in base al loro carattere riservato, od al loro rilievo per le funzioni pubbliche¹⁷⁷.

Ove secondato, tale orientamento potrebbe escludere la necessità del ricorso a forme di tutela proprie dei beni materiali anche verso le informazioni od i dati « in sé » considerati.

5. *La cancellazione del contenuto dei dati e dei programmi nell'ordinamento americano.*

Osservazioni in parte analoghe a quelle che precedono possono essere formulate in tema di cancellazione dei dati o dei programmi realizzata senza che il supporto in cui essi si trovano incorporati resti danneggiato. Il reato di *mischief*, nei diversi ordinamenti statunitensi, si presenta, infatti, strettamente correlato alla tutela dei beni materiali e dunque inapplicabile ai fatti che interessano¹⁷⁸.

È per tale ragione, e per evitare che condotte oltremodo dannose risultino penalmente indifferenti, che nella legislazione adottata da taluni Stati per combattere la criminalità informatica, il *damage* doloso ai dati od al *software* è assunto a rilevanza criminale.

Come già si è potuto considerare riguardo all'accesso abusivo od al furto di servizi, anche la condotta di danneggiamento dei dati e dei programmi è stata assunta nella legislazione statale a diversi livelli: come elemento costitutivo d'una fattispecie più complessa

¹⁷⁵ Interessa qui segnalare che sono puniti l'apprensione o la rivelazione di dati solo se concernono informazioni riservate o costituenti segreto industriale. Il contenuto delle disposizioni penali, sui dati, emesse dallo Stato del Missouri è analogo (Mo. Ann. Stat. 569-093-5).

¹⁷⁶ Sulla disciplina penale del segreto in-

dustriale negli S.U. cfr. G. THACKERAY, *op. cit.*, p. 310; U.S. DEPARTMENT, *cit.*, p. 2; ed estesamente A. ALESSANDRI, *op. cit.*, p. 149 ss.

¹⁷⁷ 18 U.S.C. 1030 (a) (1-3) riportati alle note: 84, 85, 86.

¹⁷⁸ Cfr. S.H. NYCUM, *op. cit.*, p. 529; U.S. DEPARTMENT, *op. cit.*, p. 2.

aggravata dal dolo specifico di frode¹⁷⁹, ovvero come reato autonomo¹⁸⁰.

A livello Federale, come per il caso di apprensione di dati, anche l'ipotesi di danneggiamento dei dati acquista penale rilevanza solo in relazione alla natura determinata delle informazioni in essi contenute¹⁸¹.

In conclusione pare essersi affermata una tendenza legislativa a livello statale alla protezione dei dati o dei programmi indifferenziata, che però non trova riconoscimento incontrastato nella giurisprudenza e nelle scelte di politica criminale sinora seguite a livello Federale.

6. *L'abusiva apprensione del contenuto di dati e programmi in relazione al sistema penale italiano.*

Nonostante le rilevanti differenze esistenti tra i diversi ordinamenti la questione della riconducibilità delle informazioni nell'ambito dei reati contro il patrimonio si è riproposta in alcuni Paesi europei come la Francia, ove tuttavia non sono state adottate soluzioni inequivocche e nette¹⁸².

Per quanto concerne l'Italia si può innanzitutto considerare che tali tendenze risultano in contrasto con la secolare evoluzione della

¹⁷⁹ Cfr. « *Whoever willfully, knowingly and without authorization destroys data, program or supporting documentation residing internal or external to a computer, computer system or network commits an offense against intellectual property* »: Fla. Stat. Ann. 815.04 (2); « *If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then...* » (ib. 815.04 (4) (b); similmente Mo. Ann. Stat. par. 569.095; 18 Pa. Cons. Stat. Ann. par. 3933; S.D. Cod. L. Ann. par. 43-43B-1 (2); La. Rev. Stat., 14, 73.5. Ariz. Crim Code 13.2316A.

¹⁸⁰ « *Any person who maliciously... damages or destroys any ...computer program or data, shall be guilty* ». Cal. Pen. Code 502 (c); e con diverse formulazioni: Ariz. Rev. Stat. Ann. par. 13-2316, R; Conn. Act of May 31, 1984 par. 2 (e); Colo Rev. Stat., par. 18-5-5-102 (2); Va. Code par. 18.2-152.4; Ill. Crim. Code, sec. 16-9 (2); Mich. Stat. Ann. par. 28 529 (5); N.M. Stat. Ann. 30-16A-4; N.C. Gen. Stat. par. 14-455 (b) (con riguardo alle informazioni esistenti, oltre che all'interno del computer, anche all'esterno di esso); R.I. Crim. Off., part. 11-52-3; Fla. Stat. Ann. par. 815.04 (2) (distruzione); Mo. Ann. Stat. par. 569.094; N.C. Gen. Stat. par. 14-455; N.D. Cent. Code par. 1516; 18 Pa. Cons. Stat. Ann. par. 3933; N.D. Cod. L. Ann. par. 43-43B-1 (2); Tenn. Code Ann. par. 39-3-1404 (b); Del. Code Ann. par. 935 (6); GA Code Ann. par.

1-9-93 (b); Idaho Code, par. 18-2202 (2); S.D. Code Ann. par. 43-43B-1 (1); Md. Crim. L. Code Ann. par. 45 (a) (solo per i dati pubblici).

¹⁸¹ 18 U.S.C. 1030 (3) *supra* nota 86.

¹⁸² Effettua una ricognizione completa degli orientamenti giurisprudenziali e dottrinari francesi, M.P. LUCAS DE LEYSSAC, *op. cit.* Ne traspaiono contrastanti indicazioni: da un lato l'esigenza di attribuire tutela alle informazioni (od almeno, a talune classi di esse); dall'altro l'inadeguatezza delle norme esistenti. Nel testo viene ampiamente commentata la sentenza *Logabax* (*Ch. Crim.*, 8 gennaio 1979; *D.*, 1979, p. 509) con cui è condannato per furto un impiegato che aveva copiato un documento riservato, ritenendosi configurato il reato nella sottrazione dell'originale per il tempo necessario alla sua copia. Si deve, però, rimarcare che la configurabilità del reato è stata pur sempre consentita dall'apprensione momentanea d'una cosa materiale: il documento originale. Per una pronuncia apparentemente analoga, cfr. *Cour de Cassation*, 29 avril 1986, *Herbreteau*, *D.*, 1987, *Jur.*, p. 131, con nota di M.P. LUCAS DE LEYSSAC. Altre considerazioni di rilevante interesse circa la proteggibilità delle informazioni sono effettuate da P. CATALA, *Ebauche d'une théorie juridique de l'information*, *D.*, 1984, *Chron.*, p. 97, e *Inf. e dir.*, 1983, I, 15; e *Id.*, *Les transformations du droit pénal de l'informatique*, in *Emergence du droit de l'informatique*, cit., p. 264 ss.

fattispecie del furto che si è andata progressivamente depurando, sino ad escludere dal suo raggio di operatività, non solo le c.d. ipotesi di furto improprio, ma anche i beni immateriali (come il contenuto delle opere letterarie) che in epoca rinascimentale erano talora stati ritenuti suscettibili di sottrazione¹⁸³.

Tuttavia l'evidente rifiorire a livello internazionale, non solo statunitense, di tentativi di ricondurre le appropriazioni dei beni immateriali (o talune categorie di essi) nell'ambito dei reati contro il patrimonio, nonché le sollecitazioni impresses dalla realtà — a causa della manifesta discrepanza tra valore economico di taluni di essi e sensibilità sociale che accompagna il relativo danno da un lato e tutela offerta nel diritto penale dall'altro — rende opportuna una seppur breve verifica dell'attuale praticabilità ed attendibilità di tali ipotesi.

Può al riguardo rilevarsi che l'applicazione della fattispecie di furto anche ai beni di natura immateriale incontra nel nostro ordinamento un primo ostacolo insormontabile nella nozione del termine « cosa », utilizzato per indicare l'oggetto materiale del reato, che, in sintonia con il significato attribuito alla parola nel parlare comune, viene riferito — come si è avuto innanzi a rilevare — esclusivamente alle cose tangibili¹⁸⁴.

Senonché anche superando l'impedimento conseguente all'oggetto materiale del reato — con soluzioni interpretative analoghe a quelle proposte in altri ordinamenti¹⁸⁵ od in Italia da una dottrina risalente¹⁸⁶ — dovrebbe rilevarsi che l'art. 624 cod. pen. difficilmente sareb-

¹⁸³ Sul « furto letterario » cfr. G. PECORELLA, voce *Furto (dir. pen.)*, in *Enc. dir.*, 1969, vol. XVII, p. 320; V. MANZINI, *Trattato del furto*, cit., p. 359. Un'interessante indagine sull'evoluzione storica della fattispecie è svolta da F. SGUBBI, *Uno studio*, cit., p. 86 ss.; ID., *Patrimonio*, cit., p. 354, il quale considera come la genericità ed estensione della figura del *furtum* fosse il frutto di una precisa scelta di politica criminale per la più ampia tutela del patrimonio.

¹⁸⁴ V. *supra*, alla nota 128. Inoltre V. D'AMBROSIO, *op. cit.*, p. 1139 rileva come sia costante l'orientamento giurisprudenziale che nega la configurabilità del furto di opere dell'ingegno.

¹⁸⁵ In ambito francese è stato di recente sostenuto che le informazioni potrebbero essere ricondotte nella nozione di energia (intellettuale) suscettibile di furto (cfr. M.P. LUCAS DE LEYSSAC, *op. cit.*, p. 639).

¹⁸⁶ Un parziale tentativo di estendere a taluni beni immateriali qualificandoli come energie umane, l'applicabilità del reato di furto venne condotto in Italia da A. DE MAR-SICO, *I delitti contro il patrimonio*, Napoli,

1951, p. 36 e L. SEVERINO, *Furto d'uso e delle energie*, Milano, 1931, p. 215, i quali, pur ritenendo di escludere dal novero delle energie passibili di furto, quelle che non possono essere distaccate dal corpo che le promana, affermano la configurabilità di tale ipotesi di reato nell'arbitraria incisione d'una rappresentazione musicale. Senonché si è contrastata tale tesi (ed inoltre quelle di portata più estesa secondo cui era ammesso il furto di energie umane ed intellettuali) rilevando che:

1) Possono ritenersi suscettive di furto esclusivamente quelle energie scindibili dal corpo che le genera, altrimenti esse non sarebbero passibili di appropriazione (cfr. V. MANZINI, *Trattato del furto*, cit., p. 356; G. PECORELLA, voce *Furto*, cit., p. 338; V. D'AMBROSIO, *op. cit.*, p. 1140; S. PUGLIATTI, *op. cit.*, p. 31).

2) Se l'energia è oggetto materiale del reato di furto, non lo sono, però, le sue manifestazioni, da cui essa ben si diversifica, sicché è inconcepibile il furto di calore o di luce (V. MANZINI, *op. ult. cit.*; G. PECORELLA, *op. ult. cit.*). Riproponendo tale assunto in ordine all'argomento che interessa, risulta

be applicabile all'attività di copia dei programmi e dei dati¹⁸⁷. L'apprensione di essi, realizzata attraverso la riproduzione, non sostanzia infatti gli elementi della sottrazione e del relativo impossessamento, necessari all'integrazione del reato: in quanto il titolare di tali beni non viene ad essere, neanche momentaneamente privato dell'originale, che resta conservato ed accessibile nella memoria dell'elaboratore. Né rispetto a tali ipotesi dovrebbe risultare applicabile la norma sul furto d'uso in relazione all'originale, ostandovi pur sempre la considerazione che si rendono a tal fine necessari lo spossessamento e la sottrazione seppur momentanei della cosa, che, neppure in tale ristretto ambito temporale, si verificano nel caso in esame.

Il ricorso a tale fattispecie ha invero consentito in passato di penalizzare alcune ipotesi di lesione dei beni immateriali, ma la sussistenza della sottrazione veniva individuata nell'avvenuta dislocazione dell'originale per il tempo necessario alla sua riproduzione. In tal modo la condotta ritenuta punibile si era sempre puntualizzata su un bene materiale, sostanzandosi formalmente in termini tradizionali¹⁸⁸. Senonché la praticabilità di tali soluzioni (con cui si ottiene un'indiretta forma di tutela dei beni immateriali) si è andata considerevolmente riducendo proprio con l'introduzione dei sistemi informatici.

Le potenzialità della nuova tecnologia hanno, in fatto, consentito di prescindere dal contatto fisico con l'originale per ottenerne la riproduzione, ed anche dalla temporanea indisponibilità dello stesso

che le informazioni, le idee, le rappresentazioni musicali, non equivalgono all'energia intellettuale, ma rappresentano, se mai le sue esplicazioni, in quanto tali insuscettibili di furto. Va, inoltre, ricordata l'opinione di A. DE MARSICO, *op. cit.*, p. 203 il quale, pur aderendo alla tesi che la copia d'un libro non realizza il reato di furto, sostiene possa raffigurarsi tale ipotesi quando si tratti d'un esclusivo ed antico volume. Non ci pare (salva la configurabilità del furto d'uso nei termini in cui dianzi si è precisato) che si possa aderire alla tesi propria dell'A. Non s'intende infatti quale elemento della concreta condotta possa intervenire a modificare la qualificazione penale, essendo il valore a tal fine indifferente.

¹⁸⁷ Escludono la configurabilità del furto di dati: C. SARZANA, *Note*, cit., p. 26; A. TRAVERSI, *op. cit.*, p. 193; e di software: F. SGUBBI, *Patrimonio*, cit., p. 370.

¹⁸⁸ Al riguardo F. CARRARA, *op. cit.*, p. 55 espone il caso d'un fotografo che arbitrariamente riprenda l'immagine d'un quadro, ritenendo non configurabile il furto se non in

relazione allo spostamento del quadro per il tempo necessario alla riproduzione. In termini analoghi: L. SEVERINO, *op. cit.*, p. 203 ss. Quanto alla configurabilità del reato di cui all'art. 646 cod. pen., nella riproduzione di opere, mentre la dottrina vi ha ravvisato un'ipotesi di appropriazione indebita d'uso non punibile, la giurisprudenza risalente è parsa talora indulgere nel ritenere integrato il reato: così Cass. Regno II, 8 ottobre 1925, in *Foro it.*, 1925, II, p. 69 (fotografo che aveva estratto, dal negativo consegnatogli per lo sviluppo, una pellicola per suo uso) od anche Trib. Milano 4 dicembre 1897, in *Monit. trib.* 188, p. 476 (il tipografo tira una copia per sé dalla composizione ricevuta). Tali sentenze sono ampiamente commentate in L. SEVERINO, *op. cit.*, p. 118. Per un'esposizione critica di altre decisioni di analogo contenuto, B. PETROCELLI, *L'appropriazione indebita*, Napoli, 1933, p. 172 ss. Sulla insussistenza dell'appropriazione indebita di opera letteraria, inoltre, C. PEDRAZZI, voce *Appropriazione indebita*, cit., p. 840.

per il titolare, così escludendo la configurabilità della sottrazione¹⁸⁹.

Si può, invece, considerare che taluni dati potrebbero ricevere tutela sussidiaria ed eventuale ricorrendo i presupposti dell'applicazione delle norme sul segreto previste dal codice penale. Fra le altre ipotesi acquista particolare rilievo la già citata norma contenuta nell'art. 623-bis cod. pen. che concerne in maniera specifica i dati informatici¹⁹⁰.

Vale tuttavia osservare che l'art. 617 cod. pen. sanzionando l'intercettazione, tutela i dati in maniera da un lato generalizzata (pre-scindendo dalla loro qualificazione o dal loro contenuto)¹⁹¹, d'altro canto relativa e cioè in quanto costituiscano l'oggetto d'una trasmissione in atto (di cui l'agente non sia destinatario). Sicché nell'attuale sistema penale è prevista una forma di tutela indifferenziata dei dati nel solo momento dinamico, mentre nessuna protezione li concerne generalmente nel momento statico, quando sono memorizzati nell'elaboratore. In tal caso potrebbero configurarsi solo le ipotesi di reato contro l'inviolabilità dei segreti in relazione ai dati che contengano notizie qualificabili come tali.

Si comprende la limitatezza della tutela così accordata alle informazioni osservando che tali norme spesso richiedono (per l'integrazione del reato) la *rivelazione* delle notizie arbitrariamente acquisite (artt. 623 cod. pen.; 620 cod. pen.); talora configurano fattispecie di *reati propri* (art. 623 cod. pen.) così circoscrivendo la punibilità del fatto¹⁹²; ed, inoltre, che in molti casi i dati sono destinati ad esser divulgati, seppur dietro compenso, tal che non è possibile qualificarli come segreti.

In conclusione si può considerare che la politica legislativa di selezionare le informazioni tutelate (in base al contenuto ed ai connotati) per quanto possa esser contestata nelle concrete e singole espressioni, in relazione alla sua limitatezza, appare preferibile rispetto all'indi-

¹⁸⁹ Quanto agli altri ordinamenti europei: per il Belgio si è ritenuto configurabile il reato di furto dei dati nella semplice attività di copia, non però nella mera lettura (J. SPREUTELS, *op. cit.*, p. 363); per la Germania si è considerato che i dati ed il *software* non sono oggetti passibili di furto (K. TIEDEMANN, *op. cit.*, p. 623). Nella 2. WIKG è stato inserito il par. 202a che punisce chi senza autorizzazione procura a sé o ad altri dati che non sono destinati a lui e che sono specificamente protetti contro l'accesso di chi non ne abbia diritto, cfr. L. PICOTTI, *La nuova, op. cit.*, p. 5. Ad analoga conclusione perviene per il diritto francese R. GASSIN, *op. cit.*, p. 38, ma si vedano anche le soluzioni proposte dagli autori citati alla nota 182 e A. MANNA, *op. cit.*, p. 503.

Inoltre cfr. U. SIEBER, *The International*,

cit., p. 53, che analizza le norme vigenti in materia in diversi Stati.

¹⁹⁰ Cfr. *supra*, par. II.

¹⁹¹ Analogamente a quanto avviene in materia di comunicazioni telefoniche, le quali sono tutelate indipendentemente dal carattere riservato del loro contenuto. Al riguardo cfr. A. CRESPI, *La tutela penale del segreto*, Milano, 1933, p. 67 s.; P. BARILE e V. CHELI, *Corrispondenza (libertà di)*, in *Enc. dir.*, vol. X, Milano, 1962, p. 743 (in part. p. 744); M. PETRONE, voce *Segreti (Delitti contro l'inviolabilità dei)*, in *Noviss. Dig.*, vol. XVI, Torino, 1969, p. 952.

¹⁹² N. MAZZACUVA, *La tutela penale del segreto industriale*, Milano, 1979, che segnala le diverse lacune esistenti nella repressione penale di tali violazioni.

stinta e generalizzata protezione dei dati che potrebbe conseguire all'adozione di soluzioni completamente diverse — come la ricomprensione dei dati nei reati contro il patrimonio — le quali comporterebbero un'estesa criminalizzazione di attività non effettivamente dannose.

7. *Cancellazione dei dati e dei programmi in Italia.*

Anche il reato di danneggiamento previsto dall'art. 635 cod. pen. richiede che l'azione dell'agente debba avere ad oggetto una cosa; tuttavia il riferimento al substrato materiale contenuto nella norma¹⁹³ potrebbe non valere ad escludere la punibilità degli atti lesivi commessi sul solo contenuto dei dati o dei programmi. A tale conclusione si potrebbe pervenire attraverso alcune considerazioni sulle modalità di attuazione delle condotte previste dalla norma incriminatrice. Se invero fra queste, la distruzione, la dissipazione ed il danneggiamento paiono non poter prescindere dal necessario coinvolgimento diretto ed immediato dei beni nel loro substrato naturalistico, diverse considerazioni potrebbero trarsi dall'ipotesi del « *render inservibile* » attraverso la quale potrebbe acquistare un certo rilievo anche il contenuto immateriale di taluni beni. È del resto noto che tale condotta consiste nell'impedire, *in conseguenza* dell'attività lesiva posta in essere, che la cosa assolva alla propria funzione, in maniera definitiva, od anche solo momentanea¹⁹⁴, sicché a seconda del valore che si attribuisca a tale locuzione, e segnatamente a seconda che essa venga interpretata in senso assoluto od in senso relativo, generico o specifico, il contenuto immateriale del supporto fisico potrebbe acquistare o meno un ruolo nell'ambito della condotta incriminata¹⁹⁵. Per esem-

¹⁹³ Anche con riguardo al reato di danneggiamento dottrina e giurisprudenza sono concordi nell'attribuire al termine « cosa » il comune significato fisico-naturalistico; V. D'AMBROSIO, *op. cit.*, p. 285; V. MANZINI, *Trattato di Dir. pen.*, cit., p. 478.

¹⁹⁴ Sulla nozione d'inservibilità, cfr. F. BRICOLA, voce *Danneggiamento*, in *Enc. dir.*, vol. XI, Milano, p. 599 (in part. p. 600); F. MANTOVANI, voce *Danneggiamento*, in *Noviss. Dig.*, vol. V, Torino, 1960, p. 112 (specif. p. 116); V. MANZINI, *op. ult. cit.*, p. 494; il quale, inoltre, rileva che il delitto di danneggiamento non consiste nell'attacco alla cosa in sé considerato, ma nel danno recato mediante una modificazione estrinseca alla cosa, tale da renderla meno pregevole o meno utilizzabile.

¹⁹⁵ Questa tesi potrebbe apparire condivisa da V. MANZINI, *op. loc. cit.*, secondo cui

l'inservibilità può sussistere anche se la cosa non abbia perso alcuna delle sue qualità o proprietà; talché il reato di cui all'art. 635 cod. pen. dovrebbe ritenersi integrato addirittura nel caso di chi mescoli i caratteri tipografici. Analogamente F. MANTOVANI, *op. ult. cit.*, p. 116 ritiene a tale titolo punibile l'alterazione delle schede d'un archivio. Riguardo allo specifico tema, L. PICOTTI, *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dati*, in questa *Rivista*, 1986, p. 969, che critica l'applicazione del reato di danneggiamento in caso di cancellazione dei dati, rilevando il pericolo connesso di cadere nell'analogia in *malam partem*, e ritenendo opportuno l'introduzione d'una specifica disposizione che tuteli i dati anche indipendentemente dal loro inserimento nel supporto.

plificare si può osservare che il supporto da cui sono stati cancellati i dati (od il programma) è in grado, se non danneggiato a sua volta, di assolvere alla funzione generica cui è destinato — e dunque di incorporare altri dati (od un altro programma) — esso non è però più in grado di rispondere alla specifica funzione cui era stato destinato dal suo titolare, e cioè di aver magnetizzati *quei* dati e *quel* programma. Si tratta sostanzialmente d'un ragionamento non diverso da quello che potrebbe effettuarsi in relazione a supporti di riproduzioni sonore o visive come le « musicassette » o le « video cassette », una volta che il loro contenuto sia stato cancellato.

È dunque attraverso un'interpretazione che rinvenga una connotazione relativa nel momento funzionale della cosa, che il suo contenuto immateriale potrebbe ricevere adeguata tutela¹⁹⁶.

Interessanti indicazioni si possono cogliere nella pur scarsa giurisprudenza di merito che di recente ha dovuto affrontare l'argomento. In primo luogo una sentenza del G.I. di Torino, in grado di appello avverso una sentenza di proscioglimento istruttorio del Pretore¹⁹⁷, ha ravvisato il reato di esercizio arbitrario delle proprie ragioni, commesso mediante violenza sulle cose, nel fatto del titolare d'una ditta di *software*, che per controversie intervenute con il concessionario d'un programma per elaboratore di contabilizzazione fiscale, ne aveva cancellato una parte, impedendo che il *software* potesse venire aggiornato secondo i mutamenti della legislazione tributaria, e così fossilizzandone l'operatività alla normativa vigente all'atto della cessio-

¹⁹⁶ Ritengono configurabile il reato di danneggiamento rispetto alla cancellazione del programma; L. TRIA, *op. cit.*, p. 288; C. SARZANA, *Note*, cit., p. 27; con appunti critici invece L. PICOTTI, *op. cit.*, p. 954; Id., *La nuova*, cit., pp. 2 e 7. Parte della dottrina tedesca aveva, con un analogo ragionamento, ritenuto punibile la cancellazione dei dati a norma del par. 303 St. G.B., che prevede il reato di danneggiamento (K. TIEDEMANN, *op. cit.*, p. 622 mentre alcune perplessità al riguardo venivano manifestate da W. HARTMANN, *La criminalité informatique et sa répression par les reformes pénales en la République Fédérale de Allemagne*, in *Dr. inf.*, 1986, *Dossier*, cit., p. 16). Nella 2 WIKG sono state inserite due norme che sanzionano il danneggiamento dei dati o programmi: il par. 303 StGB, che punisce chi rende inutilizzabile o manomette dati e il par. 303b StGB che punisce chi disturba un procedimento di elaborazione dati che sia di significato essenziale per un'azienda od impresa o per una pubblica amministrazione, provocando anche la distruzione, manomissione, inutilizzabilità d'un supporto informatico, al riguardo

L. PICOTTI, *La nuova normativa*, cit., p. 14, 5. Nell'ordinamento francese si è esclusa la configurabilità del reato di danneggiamento (art. 434 code pén) stante il carattere intangibile dei dati e dei programmi, e si è ritenuta applicabile solo la contravvenzione di danneggiamento della proprietà mobiliare (R 38, VI) di cui si è segnalata la risibilità delle pene (P. SARGOS, M. MASSE, *op. cit.*, p. 22; R. GASSIN, *op. cit.*, p. 37); per quanto riguarda l'ordinamento belga C. ERKELENS ha rilevato l'affinità del fatto in questione con i reati di falso per soppressione, piuttosto che con il danneggiamento (*op. cit.*, p. 28).

Per un'esposizione dell'argomento in relazione a diversi Stati occidentali cfr. U. SIEBER, *The International*, cit., p. 78.

¹⁹⁷ Sent. Uff. Istruzione Torino, 12 dicembre 1983, BASILE, in *Giur. it.*, 1984, II, p. 351, con nota di A. FIGONE, *Sulla tutela penale del software*. Nella sentenza pretorile appellata si era esclusa la configurabilità del reato di danneggiamento, data l'irriducibilità del contenuto dei programmi alla nozione di cosa.

ne. Quanto interessa evidenziare è che attraverso tale pronuncia si è ritenuta configurabile la « violenza sulle cose » anche se indirettamente esercitata, cioè senza un immediato coinvolgimento del programma, il cui supporto, oltre a risultare integro, era ancora in grado di assolvere parzialmente la sua funzione specifica¹⁹⁸.

In un caso ancor più recente si è contestata da parte del P.M.¹⁹⁹ la speciale ipotesi di danneggiamento prevista dall'art. 420 cod. pen., per gli attentati ad impianti di elaborazione di dati, nel caso di una parziale cancellazione del programma, che pare avesse avuto come esito di impedire all'impianto dell'università in cui operava di funzionare regolarmente.

Se il processo in questione si è risolto con il proscioglimento dell'imputato per non aver commesso il fatto — senza che nella sentenza venisse, per l'assorbente ragione dell'estraneità dell'imputato, presa in considerazione l'astratta configurabilità del reato²⁰⁰ — anche in tale situazione l'imputazione elevata attribuiva penale rilevanza alle conseguenze derivate dalla cancellazione del programma alla funzionalità dell'impianto, con un ragionamento non diverso da quello che si è dinanzi svolto²⁰¹.

8. *La falsificazione dei dati. Considerazioni introduttive e disciplina dell'alterazione dei dati e dei programmi negli Stati Uniti.*

L'ordinamento statunitense si è interessato anche all'aspetto diverso dell'integrità e veridicità dei dati; rivelatosi di importanza centrale, in quanto diversi comportamenti illeciti, fra cui alcuni modelli ormai classici di frodi informatiche, sono stati preceduti dalla « falsificazione » dei dati memorizzati nell'elaboratore²⁰².

L'argomento merita perciò attenta considerazione sia perché la manipolazione dei dati può divenire una condotta economicamente dannosa in quanto prodromica ad altre attività illecite, ma anche perché i c.d. *hackers* la praticano senza perseguire ulteriori finali-

¹⁹⁸ Secondo L. PICOTTI, *La falsificazione*, cit., p. 954 nella sentenza, l'elemento della violenza sulla cosa non è identificato in una precisa modalità della condotta.

¹⁹⁹ Cfr. la sentenza relativa al procedimento (G.I. Firenze 27 gennaio 1986, PASQUI, *Foro it.*, 1986, II, p. 359, con nota di C. RAPISARDA; nonché in questa *Rivista*, 1987, p. 969, con nota di L. PICOTTI, *La rilevanza*, cit.).

²⁰⁰ Non pare che la sentenza del G.I. rispecchi la massima pubblicata, ed invero mentre in quest'ultima si ritiene affermata la configurabilità del reato di cui all'art. 420

cod. pen. nel fatto di chi, attraverso la cancellazione dei programmi, abbia provocato l'interruzione del centro di elaborazione dati dell'Università, la sentenza non si pronuncia sulla correttezza della contestazione da parte del P.M.

²⁰¹ C. RAPISARDA, *op. cit.*, p. 361.

²⁰² Sulle tecniche di manipolazione dei dati cfr. L. PICOTTI, *La falsificazione* cit., p. 944 ss; U.S. DEPARTMENT OF JUSTICE, *Criminal Justice*, cit., pp. 9, 5; W.H. HYMAN, *op. cit.*, p. 524 ss.; WHITE COLLAR CRIME, *A Survey*, cit., p. 374; J.T. SOMA, *op. cit.*, p. 266 ss.

tà²⁰³. Alla distinzione di intenti associati all'alterazione delle informazioni memorizzate, si sono riferiti i legislatori statali nelle leggi in materia di criminalità informatica prevedendo due distinte fattispecie di reato. L'una rappresentata dal mero fatto di alterare i dati, elevato ad autonoma ipotesi di reato²⁰⁴, l'altra consistente nella medesima condotta accompagnata dall'intento di commettere o progettare un ulteriore reato informatico, come la frode, oppure di procurarsi denaro od utilità²⁰⁵. In maniera indipendente è stata qualificata l'inserzione dei dati senza autorizzazione, che viene considerata come una modalità di accesso abusivo²⁰⁶.

In entrambi i casi si realizza, dunque, una significativa anticipazione della sfera di punibilità, che risulta molto arretrata nel caso di autonomia e di indipendenza della fattispecie di alterazione di dati. Una tutela che può apparire sino eccessiva se la stessa legge definisce il termine elaboratore in maniera estesa non escludendone i dispositivi meno sofisticati.

In tal caso infatti le pene previste per l'alterazione dei dati sarebbero applicabili anche alla modifica di indirizzi contenuti in una agendina informatica ancorché non abbia determinato conseguenze giuridicamente rilevanti.

A livello Federale, è stata, invece, sanzionata l'alterazione di talune categorie di dati²⁰⁷. In assenza di una legislazione speciale potrebbe configurarsi nell'attività di alterazione dei dati il reato statale di *forgery* (falso), anche se per lo più solo nei casi in cui consegua ad essa l'emissione di *output* ed in particolare di *asegni*²⁰⁸.

²⁰³ I. MURPHY, *op. cit.*, p. 25.

²⁰⁴ « Any person who maliciously... alters any ...computer program or data, shall be guilty... » (Cal. pen. Code 502 (c). Le disposizioni di legge degli altri Stati sono le medesime citate alla nota 180.

²⁰⁵ « Whoever willfully knowingly and without authorization... alters data, programs or supporting documentation residing internal or external to a computer, computer system or network... » (Fla. Stat. Ann. Par. 815.04 (7); « If the offence is committed for the purpose of devising or executing any scheme or artifice to defraud or obtain any property » (id. 815.04 (4). Per le altre disposizioni statali di analogo contenuto cfr. nota 179.

²⁰⁶ Cfr. *supra*, par. II.

²⁰⁷ V. U.S.C. 1030 (a) (3) riportato alla nota 87.

²⁰⁸ V. U.S. DEPARTMENT OF JUSTICE, *Legislative resource*, cit., p. 8; S. SCHOL-

BERG, *op. cit.*, p. 77; A. BEQUAI, *op. cit.*, p. 34, i quali rilevano che, a livello statale spesso la presenza d'uno scritto è essenziale per l'esistenza di un falso punibile. Nel sistema federale non è prevista a livello legislativo una generale incriminazione del falso, ma vengono punite solo alcune falsificazioni su determinati documenti (*false entry*) cfr. A. BEQUAI, *op. cit.*, p. 40.

La dottrina statunitense non ha comunque dedicato molta attenzione alla fattispecie di falsificazione dei dati. Il più noto caso è stato deciso con la sentenza U.S. v. JONES, 414, F. Supp., 964 (D.MD, 1979); 553 F2d, 251 (4th Cir.), *Cert. denied*, 431 U.S. 968 (1977). L'imputato era riuscito ad ottenere, mediante l'immissione di dati falsi, l'emissione di assegni per rilevanti importi da parte del computer. Non essendo i titoli di credito emessi da una pubblica autorità, la qualificazione penale del fatto di alterazione ha interessato la giurisdizione federale solo per ve-

9. La falsificazione dei dati in Italia.

In Europa la questione della tutela della veridicità dei dati ha destato gravi preoccupazioni, in quanto la normativa penale posta tradizionalmente a sanzione delle falsità documentali risulta per lo più inapplicabile ai dati memorizzati; tanto che in Germania si è considerato opportuno introdurre una nuova fattispecie di reato: il falso in dati rilevanti a scopi probatori²⁰⁹.

In Italia, affrontando la questione sotto il profilo interpretativo delle vigenti norme sul falso, si è giunti a prospettare la conclusione che l'attività di falsificazione dei dati memorizzati non sia penalmente sanzionabile nella quasi totalità dei casi²¹⁰. Le ipotesi si distinguono nettamente a seconda della fase del processo di elaborazione in cui si inserisce l'attività di alterazione.

Invero nel corso delle fasi di emissione e di trattamento i dati sono fissati nella memoria dell'elaboratore in forma di impulsi elettronici, sicché non presentano le caratteristiche proprie dei documenti penal-

rificare la sussistenza del presupposto del reato di Interstate transportation of stolen goods. In primo grado questa venne esclusa, in quanto l'alterazione venne qualificata come *forgery*, che non costituisce presupposto del reato previsto dal par. 2314, in secondo grado, invece, si ritenne che la manipolazione costituiva frode, e l'attività successivamente posta in essere dall'imputato venne ritenuta punibile. Sulla sentenza WHITE COLLAR CRIME, *A survey*, cit., p. 377; E. HYMAN, *op. cit.*, p. 528, che svolge una particolareggiata ricostruzione del fatto; M.D. SCOTT, *op. cit.*, par. 8.8.

²⁰⁹ K. TIEDEMANN, *op. cit.*, p. 620 aveva originariamente rilevato che la configurabilità dei reati di falso comune previsti dal codice penale tedesco (par. 267 StGB) era interdetta dall'assenza nei dati memorizzati dei requisiti previsti per l'integrazione delle fattispecie, in particolare dell'incorporazione in carta, della leggibilità, della sottoscrizione; negli elaborati, che invece presentano tali requisiti, verrebbe a mancare la destinazione alla circolazione giuridica (altresì necessaria alla perfezione del reato) ove essi fossero destinati all'uso all'interno di un'impresa. Nel progetto per la seconda legge contro la criminalità economica era proposta l'introduzione del reato di falso in dati memorizzati (par. 269 StGB) il cui testo è stato riportato in appendice a K. TIEDEMANN, *op. cit.*, p. 633, e C. SARZANA, *Note*, cit., p. 28, con esso si intendeva punire il fatto se finalizzato alla commissione di frodi, con una scelta non diversa da quella effettuata da taluni Stati americani.

Nella 2 WIKG si è, invece, rivoluzionata l'ottica del progetto, sanzionando con il nuovo par. 267 StGB la condotta di chi « al fine d'inganno nei rapporti giuridici memorizza o modifica dati rilevanti a fini probatori, in modo tale che in caso di loro lettura equivarrebbero ad un documento autentico ovvero falsificato », cfr. L. PICOTTI, *La nuova normativa*, cit., pp. 17, 5. P. SARGOS e M. MASSE, *op. cit.*, p. 30; P. GASSIN, *op. cit.*, p. 40 ritengono che l'alterazione dei dati non sia punibile per mancanza del requisito della scrittura J. PRADEL e C. FEUILLARD, *op. cit.*, p. 310, pur convenendo, in linea generale, considerano punibili le falsificazioni incidenti sugli elaboratori. Per il Belgio analoghe considerazioni sono proposte da C. ERKELENS, *op. cit.*, p. 25 e da J. SPREUTELS, *op. cit.*, p. 193. Rileva L. MENNELLY, *op. cit.*, p. 558 il diverso orientamento della giurisprudenza inglese, che avrebbe, con l'usuale pragmatismo, trattato l'alterazione dei dati informatici come falso realizzato con i mezzi tradizionali.

²¹⁰ C. SARZANA, *Note*, cit., p. 28; ANGE-
LUCCI, in *Tavola rotonda*, INFORAV, cit.,
p. 207. Giunge a tale conclusione dopo
un'approfondita ricognizione, ricca di richia-
mi alla dottrina tedesca sull'argomento L. PI-
COTTI, *La falsificazione*, cit. Perviene a con-
clusioni distinte a seconda della fattispecie
penale da applicarsi, G. MARINI, *Condotte di
alterazione del reale aventi ad oggetto nastri e
supporti magnetici e diritto penale*, in *Riv.
dir. proc. pen.*, 1986, p. 381.

mente considerati²¹¹: quali l'incorporazione in un supporto cartaceo, la comprensibilità da parte di un uomo e la sottoscrizione²¹² (che consente il riferimento della paternità dell'atto), e perciò non sono riconducibili al tipico oggetto del falso. Né l'apparizione dei dati sullo schermo del terminale porterebbe rilevanti modifiche alla qualificazione del fatto, poiché rimarrebbe insussistente il requisito dell'incorporazione in carta, pur presentandosi quello della scrittura in forma umana²¹³. Anche con l'emissione degli elaborati scritti su carta, potrebbe non risultare presente che in un numero esiguo di casi la sottoscrizione, o, comunque, il requisito della riconoscibilità dell'autore²¹⁴. Ove per taluni elaborati venisse imposto da una disposizione espressa un particolare regime, che comprenda l'obbligo di sottoscriverli²¹⁵, si potrebbe, invece, configurare il reato di falso. In tali situazioni già l'immissione di falsi dati potrebbe risultare penalmente perseguibile a titolo di tentativo di falso, ricorrendo l'elemento soggettivo e gli altri presupposti per la sua configurabilità²¹⁶.

Dovrebbe, tuttavia, esser apprestata una più incisiva tutela della veridicità dei dati, o meglio di taluni di essi, considerato che rappresentano una forma di conservazione di atti giuridicamente rilevanti d'impiego ormai frequente, data la maggiore praticità che presenta rispetto all'archiviazione in supporti cartacei. L'opportunità di introdurre una fattispecie di reato per sanzionare il falso nei dati informatici, dovrebbe comunque esser attentamente valutata, con riguardo soprattutto alla selezione dei dati che meritano la tutela penale o dei fatti di cui è opportuna la sanzione; tale scelta potrebbe esser condotta secondo diversi criteri, considerando la natura dell'atto che sono destinati a rappresentare, oppure, l'intento che l'agente persegue attraverso l'alterazione²¹⁷.

²¹¹ Secondo un orientamento dottrinario invalso, la nozione giuridica di documento non si esaurisce nel novero di quelli contemplati dalla normativa penale nei reati contro la fede pubblica. Il documento in senso lato è nozione più estesa in cui potrebbero venir compresi anche i dati memorizzati, ove si acceda alla tesi che essenziale all'esistenza del documento è solo la sua attitudine a rappresentare un fatto, v. al riguardo F. CARNELUTTI, *Teoria del falso*, Padova, 1935, p. 138 ss. il quale riteneva di includere nella nozione di documento anche le riproduzioni fonografiche e cinematografiche; si veda analogamente: P. GUIDI, *Teoria giuridica del documento*, Milano, 1950, p. 45. Ritene G. MARINI, *op. ult. cit.*, p. 390 s. che i dati memorizzati non possono qualificarsi quali atti pubblici penalmente rilevanti; ne che le tessere o i documenti di riconoscimento magnetici possano esser considerati contrassegni e tutelati dalle relative norme penali.

²¹² L. PICOTTI, *op. cit.*, p. 954.

²¹³ *Op. loc. cit.*

²¹⁴ In merito alle difficoltà esistenti per individuare l'autore del documento informatico L. PICOTTI, *op. cit.*, p. 956.

²¹⁵ L. PICOTTI, *op. cit.*, p. 955 il quale considera, inoltre, che in tal modo la tutela penale sia tardiva e solo eventuale.

²¹⁶ La configurabilità del tentativo dei reati di falso è questione sinora discussa, cfr. per tutti F. ANTOLISEI, *Manuale*, parte II, cit., p. 577, il quale non ne esclude la ricorrenza. Tuttavia, pare che l'introduzione dei sistemi informatici consentendo il trascorrere d'un lasso di tempo fra l'azione del soggetto e l'inserzione dei falsi dati, che può esser oggettivamente considerata come atto inequivoco diretto alla produzione del falso, e l'effettiva consumazione del reato, conduca nuovi argomenti a sostegno della tesi favorevoli alla sussistenza del tentativo. Allo specifico riguardo del tentativo nelle alterazioni informatiche cfr. G. MARINI, *op. cit.*, p. 395.

²¹⁷ La prima soluzione è stata prescelta, come si è visto, nell'ordinamento federale americano (18 U.S.C. 1030 (a) (3); la seconda

IV. FRODI INFORMATICHE

1. *Nozioni e tecniche.*

Alcune ricerche statistiche condotte negli Stati Uniti hanno rivelato che le frodi informatiche costituiscono una delle manifestazioni di maggior rilevanza economica della criminalità da *computer*²¹⁸. Tale valutazione potrebbe apparire più preoccupante ove si consideri che si fonda sull'analisi dei soli episodi denunciati, i quali (per il c.d. fenomeno del numero oscuro²¹⁹ dei reati informatici) rappresenterebbero una esigua percentuale di quelli effettivamente perpetrati.

Può innanzitutto precisarsi che il termine frodi informatiche è utilizzato in senso aspecifico per indicare quei casi in cui, attraverso l'indebito uso d'un elaboratore, si ottiene una disposizione patrimoniale cui non si abbia diritto.

Questo settore dei reati informatici riguarda in misura principale, ma non esclusiva, due tipi di sistemi di elaborazione dati, attraverso i quali si può agevolmente perpetrare un'attività fraudolenta: in primo luogo i centri che operano il trasferimento elettronico di fondi (c.d. « EFT ») ed inoltre i sistemi di elaborazione in uso ad enti od imprese adoperanti allo scopo di memorizzare i dati relativi agli obbligati od agli aventi diritto a prestazioni patrimoniali²²⁰.

Le diverse suddivisioni proposte in materia, fondate sulla base di rilevazioni empiriche, consentono innanzitutto di distinguere i diversi episodi verificatisi secondo il particolare metodo prescelto dall'autore per ottenere l'indebito vantaggio economico. In primo luogo la disposizione patrimoniale può conseguire all'accesso abusivo all'elaboratore; come è avvenuto nei casi in cui l'agente, procuratosi una tessera per attivare l'elaboratore di un istituto di credito, si sia limitato ad ottenere la consegna di somme depositate presso un conto ad altri intestato²²¹.

invece è seguita dai compilatori del progetto di legge tedesco, per cui v. *supra*.

²¹⁸ J.K. TABER, *op. cit.*, p. 276 citando altre fonti quantifica in 78 milioni di dollari i danni sino allora conseguenti alle frodi derivanti da altri illeciti, cui inoltre sono da aggiungere i 2 miliardi di dollari derivanti dalla sola frode dell'*Equity Funding corp.* (falsificazione di 64.000 polizze assicurative) per cui v. S.H. NYCUM, *op. cit.*, p. 527. Si vedano inoltre i prospetti statistici pubblicati da K. TABER, *op. cit.*, redatti dall'*Institute for the Future* (p. 278) e dal *General Accounting Office* (p. 285 ss.) che offrono un interessante e completo quadro dei danni economici prodotti dai diversi tipi di *computer crime*.

²¹⁹ Tale fenomeno, segnalato da D.B. PARKER, *Computer, cit.*, p. 16, è stato pacifi-

camente riconosciuto dagli autori che si occupano di criminalità informatica. Sulle cause determinanti cfr. S.L. SOKOLIK, *op. cit.*, p. 539. Secondo L. WHARTON, *op. cit.*, p. 239 solo il 9% dei criminali informatici viene scoperto e solo il 15% di questi viene denunciato.

²²⁰ G. MONALDO e G. VALLERANI, *op. cit.*, p. 191 segnalano fra gli altri che un ambiente favorevole alle frodi informatiche è quello in cui vengono svolti processi ripetitivi; in tal senso anche U. SIEBER, *The International*, cit., p. 13.

²²¹ Si tratterebbe in maniera particolare delle frodi al Bancomat realizzata attraverso l'uso di tessere d'accesso da parte d'una persona non legittimata. Circa il funzionamento del sistema Bancomat v. F. MAIMERI, *Servi-*

Inoltre, una frode informatica può essere perpetrata attraverso la manipolazione dei dati memorizzati nell'elaboratore. A tale categoria appartengono i ricorrenti episodi in cui, attraverso l'inserimento di dati non veritieri nella memoria dell'elaboratore, figurano adempiute le obbligazioni patrimoniali a carico dell'agente (quali i contributi o le rate dovuti) di modo che non ne venga più sollecitato il pagamento; oppure, risultano dovute per destinatari fittizi alcune prestazioni patrimoniali periodiche (come ad es. stipendi o pensioni) che vengono, invece, ricevute, dagli autori del fatto, od ancora, si rappresenta una situazione di solvibilità tale da legittimare l'accensione dei mutui richiesti²²².

Si possono infine attuare le frodi informatiche impiegando tecniche ancor più sofisticate, attraverso interventi di modificazione dei programmi anche (ma non necessariamente) combinati con manipolazione di dati. Diverse sono le tecniche sinora maggiormente utilizzate: la più semplice è quella c.d. del « salame », consistente nell'intervento sul programma sicché al momento del calcolo degli interessi bancari venga sottratta una minima percentuale dalla somma dovuta a ciascun correntista e la differenza sia convogliata su un unico conto, il quale viene così a beneficiare di ingenti versamenti. Più complesso è il sistema del c.d. « cavallo di Troia », e cioè dell'inserimento nel programma operativo d'una serie di istruzioni supplementari, inaccessibili a persone diverse dall'autore della manipolazione²²³.

2. Qualificazione dei fatti nell'ambito del sistema federale americano: attualità e proposte.

Negli S.U. la perseguibilità penale di questi comportamenti è stata garantita, quantomeno a livello Federale attraverso l'applicazione della preesistente normativa e non ha dato luogo a particolari proble-

zio Bancomat, in *Contratti bancari*, in *Leg. econ.*, 1982-1983, Milano, 1985, 146 ss., G.L. BRANCADORO, *Profili di responsabilità contrattuale ed aquiliana della banca nell'erogazione servizio Bancomat*, in questa *Rivista*, 1985, p. 651 ss.; G. CORRIAS LUCENTE, *Bancomat e responsabilità per l'abuso del correntista*, *ivi*, 1985, p. 720, descrivono la struttura di tali frodi con attenzione K. TIEDEMANN, *op. cit.*, 619, il quale è restio a considerarle fra i *computer crime*; W. JEANDIER, *Les truquages et usages frauduleux de cartes magnetiques*, in *J.C.P.*, 1986, 1 ss.; J. PRADEL e C. FEUILLARD, *op. cit.*, p. 312.

²²² Cfr. R.D. NORMAN, *op. cit.*, p. 72; U.S. v. ALSTON, 609, F2d, 531; WHITE COLLAR CRIME, *A survey*, p. 378 ss.; Id., *Second survey*, p. 499.

²²³ Una descrizione molto accurata sotto il profilo tecnico di alcuni casi e sistemi di frodi informatiche è effettuata, J.K. TABER, *op. cit.*, p. 311 ss., e sui sistemi di manipolazione dei programmi da H. HYMAN, *op. cit.*, p. 525 ss., inoltre v. T.J. SOMA, *op. cit.*, p. 272; WHITE COLLAR CRIME, *op. cit.*, p. 375, nt. 1744; D.B. PARKER, *Computer*, *cit.*, p. 84; Id., *The computer criminal: motivations and modus operandi*; Rel. Ced., *cit.*, pp. 2, 5; M.D. SCOTT, *op. cit.*, par. 8.9; U.S. DEPARTMENT, *Criminal Justice*, *cit.*, p. 9 s.; L. TRIA, *op. cit.*, p. 286. Sulle possibilità di tipizzare alcuni episodi e sulle relative iniziative per la prevenzione e la scoperta v. G. MONALDO e G. VALLERANI, *op. cit.*, p. 279 ss.; U. SIEBER, *The International*, *cit.*, p. 6.

mi. Si è segnatamente ritenuto che le frodi informatiche possano integrare i reati di « *wire fraud* »²²⁴ e « *mail fraud* »²²⁵. La condotta prevista da tali norme incriminatrici (come si è precedentemente esposto in materia di *mail fraud*) è descritta in termini alquanto generici così da risultare scarsamente tipizzata: per integrare il reato è, infatti, sufficiente che l'autore agisca per eseguire o progettare un piano fraudolento, facendo uso della posta o di cavi, in comunicazioni dirette verso uno Stato diverso da quello di partenza, ovvero verso uno Stato estero²²⁶.

Si possono in tal modo cogliere le rilevanti differenze esistenti fra le ipotesi di truffa previste in alcuni sistemi di *civil law* e le fattispecie statunitensi, che prescindono sia dall'acquisito vantaggio patrimoniale in capo all'agente, che dal pregiudizio economico della parte offesa, sia dall'induzione in inganno di una persona²²⁷. Intuitivamente si comprende come le figure di reato federali presentino una maggiore duttilità, che consente l'applicazione delle norme agli indicati casi di frodi informatiche; tale esito è reso agevole dalla previsione, quale requisito del reato, dell'uso di cavi di comunicazione nel cui novero sono riconducibili, senza necessità di ricorrere ad artifici interpretativi, anche gli strumenti tecnici che connettono le diverse componenti di un sistema di elaborazione di dati²²⁸.

Né la terminologia tecnica, né la struttura delle fattispecie astratte si sono rivelate, dunque, d'ostacolo all'applicabilità di tali norme anche alle frodi informatiche. L'unico tramite alla loro piena efficacia deriva invero dall'imposizione del requisito spaziale, sicché ove l'uso dei casi resti circoscritto all'interno d'un unico Stato, non si potrebbe, dati i termini contenutistici della competenza Federale, ravvisare il reato di *wire fraud*²²⁹.

Si è però precisato²³⁰ che quantomeno l'attività diretta all'illecita appropriazione di denaro o valori appartenenti al Governo o ad uffici

²²⁴ 18 U.S.C. par. 1342 « *Whoever having or intended devise any scheme or artifice to defraud or for obtaining money or property by means of false or fraudulent pretenses... transmits or causes to be transmitted by means of wire any writing, signs, signals, pictures, or sounds, for the purpose of executing such scheme or artifice...* ».

²²⁵ Il testo è già riportato *supra*, alla nota 167.

²²⁶ Sulla struttura di tali reati, v. WHITE COLLAR CRIME, 3d Annual, cit., p. 281 ss., per taluni aspetti particolari che vengono sottoposti ad attento studio cfr. J.B. COFFEE, *op. cit.*

²²⁷ Un'interessante analisi in termini comparatistici delle disposizioni sul reato di

truffa negli ordinamenti europei è svolta da G. MARINI, *Truffa*, cit., p. 865. In generale sul reato di Fraud negli S.U. cfr. K. SCHULHOFER PAULSEN, *op. cit.*, p. 942.

²²⁸ Così G. THACKERAY, *op. cit.*, p. 305; M.D. SCOTT, *op. cit.*, par. 8.9; A. BEQUAI, *Computer*, cit., p. 37; WHITE COLLAR CRIME, *Survey*, cit., p. 371; 2nd, p. 501; 3d, p. 281.

²²⁹ L.I. KRAUSS e A. MAC. GAHAN, *op. cit.*, p. 311; A. BEQUAI, *Computer*, cit., p. 38.

²³⁰ U.S. DEPARTMENT OF JUSTICE, *op. cit.*, p. 11; D.B. PARKER, *Computer*, *op. cit.*, p. 85; A. BEQUAI, *How to prevent*, cit., p. 18; M.D. SCOTT, *op. cit.*, 8.13.

Federali — ove non configuri i reati di frode — potrebbe venir sanzionata attraverso l'*Embezzlement and Theft Statute*²³¹.

Nonostante le diverse possibilità di qualificazione penale del fatto si è da parte di taluno avvertita l'opportunità di emanare una disposizione specifica, anche per inasprire le sanzioni applicabili alle *computer frauds*²³², ed allo scopo sono stati presentati diversi progetti di legge, nessuno dei quali è stato sinora approvato. Nel testo proposto nel 1977 (S. 240) — e per tale parte recepito inalterato nel progetto depositato nel 1981 (H.R. 1092) — si è proposta l'introduzione del reato di accesso abusivo ad un elaboratore appartenente al Governo o ad uffici Federali con lo scopo di:

- a) progettare od eseguire un piano di frode;
- b) ottenere denaro o proprietà²³³.

Come si può rilevare, la fattispecie che parzialmente riproduce lo schema dei reati di *mail e wire fraud*, s'incentra sulla condotta di accesso abusivo all'elaboratore, qualificata dallo specifico dolo, consistente nell'intervento di commettere (od anche solo di progettare) una frode od ottenere utilità, di modo che la punibilità del fatto è significativamente anticipata rispetto al raggiungimento dello scopo proposti dall'agente.

3. *Trattamento penale nell'ambito dei singoli Stati americani.*

Esaminando la varia legislazione statale in materia di frode, si è invece, considerato che le singole norme incriminatrici risultano spesso inoperanti rispetto a talune ipotesi di frodi informatiche; in quanto richiedono, quale elemento necessario all'integrazione del reato, l'avvenuto inganno d'una persona, che non si potrebbe ravvisare nelle false indicazioni (od ordini) forniti ad una macchina²³⁴.

Taluni Stati hanno ovviato all'ostacolo rappresentato da tale requisito attraverso emendamenti legislativi, che espressamente includono fra i mezzi tipici di realizzazione del fatto anche le false rappre-

²³¹ Il testo del 18 U.S.C. par. 641 è riportato *supra*, alla nota 81.

²³² Le pene risultano, infatti, duplicate, per maggiori dettagli al riguardo v. *infra*, par. VII.

²³³ S. 240 (proposed) 18 U.S.C. par. 1028 (1) (a). *Whoever knowingly and willfully directly or indirectly, accesses, causes to be accessed or attempts to access any computer, computer system or network... which, in whole or in part operates in interstate commerce, or is owned by, under con-*

tract to, or in conjunction with any financial institution, the U.S. government or any branch, department, or agency thereof, or any entity operating or affecting interstate commerce for the purpose of: 1) devising or executing any scheme or artifice to defraud or 2) obtaining money property or service, for themselves or another by means of false or fraudulent pretenses, representations or promises » (il testo è riportato in 2 *Computer L.J.*, 1980, p. 722).

²³⁴ L. WHARTON, *op. cit.*, p. 247.

sentazioni dirette ad un elaboratore²³⁵, per quanto anche in via interpretativa della normativa esistente potrebbe stabilirsi che non rappresenta una giustificazione valida ad inficiare l'accusa l'affermazione che il soggetto passivo dell'inganno è rappresentato da una macchina e non da una persona²³⁶.

Nel contesto del processo di legiferazione della materia dei *computer crime*, alcuni Stati hanno inoltre introdotto disposizioni concernenti specificamente il reato di frode informatica. Le fattispecie previste in tali leggi presentano una struttura in parte analoga a quella descritta nel progetto Federale e dianzi riportata. Peraltro esse possono venir ricondotte a due modelli principali distinguendole a seconda delle modalità previste per la realizzazione del fatto tipico, talune disposizioni identificando la condotta nel solo accesso abusivo²³⁷, altre invece considerando anche l'alterazione di dati o programmi²³⁸. Può agevolmente rilevarsi che anche sulla base di tali disposizioni la potestà punitiva può essere esercitata in una fase antecedente alla causazione del danno.

4. Rilevanza penale delle diverse fattispecie in Italia.

Contrariamente a quanto è avvenuto nel sistema Federale americano, nell'ambito dell'ordinamento italiano, invece, la questione della qualificazione penale degli illeciti dianzi descritti e denominati frodi informatiche è risultata, alla luce della vigente normativa, alquanto complessa.

Nel tentativo di ricondurre tali fattispecie nello schema tipico del reato di truffa si è rivelato che in molte di esse viene a mancare l'induzione in errore di taluno richiesto come elemento necessario all'integrazione del reato previsto dall'art. 640 cod. pen.²³⁹.

²³⁵ « For an offense that requires "deception" as an element it is not a defense that the defendant deceived or attempted to deceive a machine » (Alaska Stat. par. 11.46.985); nella disposizione sulla *computer fraud* in Utah si sono espressamente incluse, tra i mezzi fraudolenti, *false representations made to a computer* » (Utah Code Ann. par. 76-6-703).

²³⁶ Cfr. L. WHARTON, *op. loc. cit.*

²³⁷ V. *supra*, nota 93.

²³⁸ V. *supra*, nota 94.

²³⁹ L. PICOTTI, *La falsificazione*, cit., p. 958; *contra*: C. SARZANA, *Informatica, Relazione C.E.D.*, cit., p. 22; *Id.*, *Reati resi possibili*, cit., p. 22; nel senso del testo: A. TRAVERSI, *op. cit.*, p. 192. Sulla non configurabi-

lità della truffa a danno delle macchine si esprimeva già V. MANZINI, *Commercio*, cit., p. 23; *Id.*, *Trattato del furto*, cit., p. 635. Invece, U. PIOLETTI, *Truffa*, in *Noviss. Dig. App.*, vol. VII, Torino, 1987, p. 907, ritiene che sia realizzato il reato di truffa: egli rileva che l'inganno si verifica in danno di colui che ha predisposto il funzionamento dell'elaboratore, ammettendo tuttavia che interviene così una sorta di « sfasamento diacronico » tra volontà, induzione in errore ed atto di disposizione (cfr. p. 912). La tesi potrebbe esser contestabile poiché in essa l'elemento dell'errore della vittima perde il connotato di effettiva realtà psicologica (talché in ipotesi l'ingannato potrebbe non essere a conoscenza dell'esistenza del negozio) per divenire una mera finzione.

Questo orientamento interpretativo, che si mostra maggioritario nel nostro Paese, si fonda sulla considerazione che il soggetto passivo dell'inganno può essere esclusivamente una persona fisica e non già una macchina. Ciò per due ordini di ragioni: per la prima, basata sull'interpretazione letterale della norma incriminatrice, si esclude che il pronome « taluno » contenuto nella norma possa indicare altro che un essere umano; per la seconda, di ordine logico, si esclude che uno stato psicologico come l'errore possa essere riferito ad un elaboratore²⁴⁰. Sulla base di tali considerazioni si è ritenuto non astrattamente configurabile il reato di truffa in tutte le ipotesi di frodi informatiche in cui la corresponsione di utilità sia direttamente effettuata dall'elaboratore senza che si verifichi il previo inganno d'una persona fisica, e, per contro applicabile la norma incriminatrice ove interven-gano delle persone impegnate al controllo delle operazioni svolte dall'elaboratore, le quali vengano indotte in errore dalla fraudolenta condotta dell'agente²⁴¹.

Riguardo a tale assunto meritano comunque di essere avanzati alcuni preliminari rilievi. Appare innanzitutto che un'estrema generalizzazione del concetto di frode informatica non possa che nuocere al tentativo di inquadrare giuridicamente tali episodi. Invero, nel novero delle frodi informatiche, termine che per ragioni meramente esemplificative è usato in senso affatto generico, sono usualmente comprese un coacervo di fattispecie concrete dalle connotazioni assai distinte, che si strutturano in maniera differente anche negli aspetti che possono assumere penale rilevanza.

Si consideri, innanzitutto, che un primo ordine di frodi informatiche può intervenire attraverso l'impiego di elaboratori che svolgono funzioni di mera memorizzazione. Essi cioè sono utilizzati per la sola attività di rappresentazione delle situazioni, mentre l'attività deliberativa ed esecutiva resta demandata ad una persona fisica. È il caso, ad esempio, dei *computer* impiegati per archiviare i dati sullo stato, finanziario delle persone al fine di valutare la concedibilità ad esse di mutui. L'alterazione dei dati concernenti la situazione patrimoniale d'un individuo, in modo da render possibile l'accensione d'un credito a suo favore, ove sia una persona a deliberare la stipula del contratto, raffigura un tradizionale reato di truffa.

In tale ipotesi, infatti, l'uso dell'elaboratore non altera la struttura tipica del fatto fraudolento, intervenendo solo nel momento di creazione degli artifici e raggiri, siccome avviene nel caso della contraffazione documentale.

²⁴⁰ L. PICOTTI, *op. ult. cit.*, *loc. cit.*

²⁴¹ Così C. SARZANA, *Note, loc. cit.*; L. PICOTTI, *op. loc. cit.* La giurisprudenza pare

aver accolto questa tesi, cfr. al riguardo Trib. Roma 20 giugno 1985, Testa, in questa *Rivista*, 1986, p. 166.

Da questo esempio, proposto a titolo meramente indicativo, si può ricavare che l'analisi della fisionomia delle diverse fattispecie di frode attraverso l'elaboratore consente di ridurre alcune di tali ipotesi alla figura tipica del reato di truffa.

Diversamente può avvenire nel caso in cui l'elaboratore svolga funzioni ulteriori rispetto alla mera documentazione, ed in particolare assolva anche a compiti esecutivi di attività negoziali. È rispetto a tali ipotesi che si incontrano i cennati limiti interpretativi alla configurabilità del reato di truffa, ravvisabile solo nel caso in cui una persona fisica sia stata indotta in inganno dagli artifici posti in essere dall'agente. Quanto al rilievo che a tal fine è sufficiente l'intervento di controlli da parte del personale va rilevato che la predisposizione di uffici deputati alla verifica dei dati e delle attività svolte dall'elaboratore può non essere sufficiente ad integrare la condizione richiesta per l'integrazione d'una truffa punibile.

Pare opportuno al riguardo considerare che gli addetti a tali uffici sono spesso incaricati di effettuare solo controlli generici, o a campione; oppure verifiche periodiche sul complesso delle attività realizzate dall'elaboratore²⁴². Può perciò accadere che tali funzionari non conoscano (o non valutino) l'esistenza ed il contenuto delle singole operazioni, e dunque non si possano considerare concretamente indotti in errore²⁴³; ovvero che prendano compiuta conoscenza della singola operazione solo dopo che la prestazione patrimoniale è stata eseguita, sicché, pur intervenendo un inganno, farebbe difetto il nesso causale fra l'errore umano artificialmente provocato e la disposizione patrimoniale²⁴⁴. Può dunque considerarsi che, anche accedendo all'interpretazione citata l'integrazione del reato di truffa verrebbe a dipendere dal concreto atteggiarsi del servizio di controllo in ciascun singolo caso: sicché la punibilità effettiva delle frodi informatiche risulterebbe ancorata ad un dato casuale ed occasionale. Il fenomeno appare del resto destinato ad accrescersi ulteriormente, in relazione alla manifesta tendenza ad una crescita esponenziale della quantità e qualità delle funzioni assegnate ad un elaboratore di dati ed alla progressiva e corrispondente riduzione del personale²⁴⁵.

²⁴² Sulle modalità di controllo più comuni, v. G. MONALDO e G. VALLERANI, *op. cit.*, p. 181 ss.

²⁴³ C. PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, p. 125 ribadisce che l'errore, dev'essere « presenza attuale d'un convincimento non conforme alla realtà », ed in consonanza a tale interpretazione dell'errore delinea il requisito

dell'atto di disposizione come « condotta fondamentalmente consapevole della propria efficacia concreta » (che nei casi di generici controlli non può essere ravvisata).

²⁴⁴ C. PEDRAZZI, *op. cit.*, p. 107.

²⁴⁵ Riconoscere la crescente « dipendenza dal computer » S.L. SOKOLIK, *op. cit.*, p. 354, che viene quantificata in *White Collar Crime*, 2nd, p. 499.

Rientra perciò nelle ragionevoli previsioni, e spesso già nella realtà, che l'intervento umano nei processi di elaborazione di dati venga limitato e circoscritto ad attività insignificanti ai fini della configurabilità del reato previsto dall'art. 640 cod. pen.

Si è per altro verso sostenuto, al fine di superare le difficoltà che si frappongono all'applicazione del reato di truffa, che si potrebbe ravvisare il diverso reato di furto con mezzi fraudolenti in talune ipotesi di frodi informatiche; e, segnatamente, in quelle attuate attraverso il sistema del Bancomat (consistenti nel prelievo di somme da parte di terzi estranei, attraverso tessere magnetiche di provenienza delittuose o contraffatte)²⁴⁶ ed in alcuni casi di indebito trasferimento di fondi attraverso i sistemi bancari²⁴⁷.

Si perviene tuttavia a tale soluzione senza affrontare alcune questioni che appaiono di determinante rilievo per la sua validità. Innanzitutto dovrebbe venir esaminata la questione concernente la sussistenza d'una sottrazione penalmente rilevante, che non appare poter essere aprioristicamente ammessa. È noto, infatti che al fine di impedire la configurabilità di tale elemento costitutivo del reato di furto è sufficiente che sia intervenuta una consegna volontaria da parte di chi vi sia legittimato, e non può apoditticamente escludersi che tale venga qualificata la consegna effettuata a mezzo dell'elaboratore e del suo terminale, considerando che esso si limita ad eseguire la volontà del suo titolare siccome predeterminata nel programma²⁴⁸.

Del resto va rilevato — e solo per comodità di trattazione si è posto questo rilievo che appare preliminare — che le due situazioni considerate si differenziano in modo giuridicamente rilevante: mentre nel prelievo attraverso gli sportelli del sistema Bancomat interviene una consegna di natura materiale (talché il richiedente acquista l'immediata disponibilità delle somme); nelle altre forme di trasferimento elettronico di fondi nell'ambito del sistema bancario²⁴⁹, non

²⁴⁶ F. MUCCIARELLI, *I computer crimes nel disegno di legge 1657/1984*, in *Riv. it. dir. proc. pen.*, 1984, 785; G. MARINI, *op. cit.*, p. 386.

²⁴⁷ L. TRIA, *op. cit.*, p. 290 riguardo alla frode realizzata con il sistema del salame. Tali ultime soluzioni rispondono all'uso, già rilevato da C. PEDRAZZI, *op. cit.*, p. 113, di ricorrere alla contestazione del furto quando nel soggetto passivo dell'inganno manca la capacità di disporre.

²⁴⁸ Cfr. G. CORRIAS LUCENTE, *op. cit.*, p. 726.

²⁴⁹ Un discorso diverso meriterebbero infatti i *Points of Sale*, cioè gli apparecchi installati presso esercizi pubblici per consentire al cliente di pagare gli acquisti attraverso

l'immediato accreditamento del relativo prezzo sul conto dell'esercente. Le frodi potrebbero esser effettuate, fra l'altro, attraverso l'uso illegittimo di false tessere. La qualificazione di tali fatti, dipende dalla regolamentazione negoziale dell'attività, che, sola, consente di individuare il danneggiato (nella banca ovvero nell'esercente) attraverso la determinazione della responsabilità contrattuale. Poiché l'installazione dei *Point of Sale*, è in Italia allo stato meramente sperimentale (e non si conosce il contenuto delle convenzioni-tipo che regolano i rapporti fra l'Istituto di Credito e l'utente o l'esercente) onde evitare esercitazioni meramente accademiche, si preferisce non trattare in questa sede l'argomento.

viene effettuata alcuna immediata consegna ma si ottiene esclusivamente che le somme siano accreditate su di un conto bancario.

Proprio il risultato che in tal caso si presenta quale esito dell'attività dell'elaboratore impone di sollevare una fondamentale obiezione alla configurabilità del reato di furto. L'agente attraverso gli artifici dispiegati (che possono variamente consistere nell'immissione di falsi dati, nell'alterazione del programma od in combinazioni di entrambe le attività) ottiene infatti il compimento d'un atto ad effetti giuridici — l'iscrizione a proprio (od altrui) credito delle somme — che può più correttamente essere attratto nell'area di tutela propria del reato di truffa piuttosto che in quella di furto. Mentre, infatti, il reato di truffa può integrarsi attraverso le varie forme assunte dalla disposizione patrimoniale del soggetto passivo, che ricomprendono l'assunzione di un'obbligazione o l'omessa richiesta del suo adempimento²⁵⁰, il reato di furto si realizza esclusivamente attraverso l'apprensione materiale d'una cosa. Ove il trasferimento reale sia mediato dall'esistenza d'un vincolo giuridico (ed avvenga in esecuzione di esso) si esorbita, pertanto, dalla fattispecie tipica del furto. La differenza insistente fra le due figure è stata delineata osservando che nella truffa l'agente informa il proprio comportamento ai modelli contrattuali (considerato che egli ottiene un trasferimento di ricchezza nel rispetto apparente delle forme negoziali proprie della società civile) mentre nel furto pone in essere un tipo di trasferimento esclusivamente naturalistico, patologico rispetto al modello contrattuale²⁵¹. Appaiono, perciò, irriducibili alla figura del furto quelle fattispecie in cui il trasferimento di fondi in capo all'agente non avviene attraverso la consegna immediata e reale delle somme effettuata dall'elaboratore, ma è realizzato attraverso l'assunzione, da parte della banca, dell'obbligazione in cui consiste l'atto di accreditamento²⁵².

²⁵⁰ Se, normalmente, le figure del furto e della truffa vengono distinte a seconda della condotta e al primo caso si rapportano solo i fatti di usurpazioni unilaterali, mentre nel secondo quei fatti realizzati mediante la cooperazione artificiosa del soggetto passivo (cfr. per tutti C. PEDRAZZI, *op. cit.*, p. 39 ss.), in questa situazione proprio le perplessità che si potrebbero sollevare in ordine all'identificazione dell'attività dell'elaboratore, con quella del soggetto passivo del reato, impone di rinvenire altrove il fondamento della qualificazione penale del fatto. Quanto alla maggior ampiezza dell'oggetto del reato di truffa, rispetto a quella del furto cfr. G. PECORELLA, voce *Furto*, cit., p. 333; Id., *Voce Patrimonio (reati)*, in *Noviss. Dig.*, vol. XXII, Torino, 1965, p. 629 (in part. p. 633); V. MANZINI, *op. ult. cit.*, p. 659. F.

SGUBBI, *Patrimonio*, cit., p. 368, ricava le differenze esistenti fra le fattispecie dei reati contro il patrimonio a seconda che la fattispecie s'incentri sulla nozione di *cosa* (come nel furto) o di *danno* come nella truffa. Riguardo alla particolare questione K. TIEDEMANN, *op. cit.*, p. 624 ha rilevato l'irriducibilità alla nozione di *cosa*, del denaro contabile, che impedirebbe di ravvisare il furto nelle citate ipotesi.

²⁵¹ F. SGUBBI, *op. ult. cit.*, p. 360.

²⁵² Sulla natura dell'atto di accreditamento v. M. PORZIO, *I contratti bancari in generale*, in *Tratt. dir. priv.* a cura di P. RESCIGNO, vol. IV, Torino, 1986, p. 876 ss.; S. MACCARONE, *Osservazioni, in tema di conto corrente bancario*, in *Le operazioni bancarie* a cura di G.B. PORTALE, Milano, 1978, p. 605 (in part. p. 641 ss.).

Se, tuttavia non si configura il reato di furto con mezzi fraudolenti per le ragioni dianzi sinteticamente esposte, il fatto che l'autore realizza un accredito delle somme attraverso l'indebito uso dell'elaboratore può essere comunque apprezzato ai fini della configurabilità del reato di truffa, anche se di per se non pare sufficiente integrarlo, in quanto ottenuto senza l'effettiva induzione in errore d'una persona. L'iscrizione delle somme a credito, procurata attraverso un'attività fraudolenta, può infatti divenire un mezzo valido per indurre in errore il dipendente della banca che debba eseguire la concreta corresponsione dell'utilità acquisita all'agente. Si tratterebbe in sostanza di considerare l'accREDITAMENTO non già come il momento conclusivo del reato ma come un aspetto degli artifici e raggiri dispiegati dall'autore per ottenere il vantaggio economico.

Né verrebbe ad inficiare la proposta soluzione, il fatto che l'accREDITO sia effettuato o spostato verso una banca diversa dall'ordinante poiché, secondo una pacifica interpretazione del reato di truffa, la persona offesa da reato ed il soggetto passivo dell'inganno non debbono necessariamente coincidere²⁵³.

Deve esser tuttavia considerato che con la costruzione delineata si realizza una considerevole posticipazione del momento consumativo del fatto rispetto alle comuni ipotesi di truffa: ed infatti l'accREDITAMENTO delle somme ottenuto mediante l'indebito uso dell'elaboratore potrebbe configurare solo un tentativo compiuto di truffa, mentre il medesimo risultato, ottenuto attraverso l'induzione in errore d'un impiegato di banca, sarebbe valido a perfezionare il reato di truffa.

Né questo appare l'unico inconveniente della costruzione proposta: v'è infatti il caso che l'agente, per realizzare le somme iscritte a suo credito, ricorra ad ulteriori transazioni attraverso i mezzi elettronici, o le prelevi mediante gli sportelli Bancomat²⁵⁴, in modo tale da render insussistente l'effettiva induzione in errore d'una persona fisica e l'ipotizzabilità del reato in questione.

La situazione che con questa breve ricognizione si è descritta rivela in conclusione l'intrinseca inadeguatezza del sistema penale a fornire una comprensiva ed omogenea risposta alle nuove tecniche truffaldine associate all'uso dell'elaboratore automatico di dati. Ancorché in

²⁵³ G. MARINI, *Truffa, ecc.*, cit., p. 370; V. MANZINI, *op. ult. cit.*, p. 643; inoltre C. PEDRAZZI, *Inganno ed errore*, cit., p. 33, p. 93 ss. che individua le condizioni necessarie perché l'atto di disposizione dell'ingannato, ove questi non sia il titolare del bene, possa esser ritenuto valido.

²⁵⁴ La crescente applicazione degli elabo-

boratori non rende, del resto, incredibile che presto molti dei compiti degli impiegati di banca verranno svolti da sportelli elettronici, sicché potrà realizzarsi l'utilità corrispondente all'accREDITAMENTO fraudolento senza entrare in contatto con una persona fisica, suscettibile d'inganno.

astratto non possa escludersi la riconducibilità dei singoli fatti nell'ambito dei reati di truffa — o di furto — previsti dal vigente codice penale, la configurabilità di tali fattispecie rimane ancorata ad evenienze accidentali ed affatto occasionali, quali l'inserzione d'un controllo umano sul contenuto dei dati immessi od emessi dall'elaboratore o le forme prescelte per il prelievo delle somme accreditate.

Né il fatto che alcune ipotesi di frodi informatiche possano sfuggire alle maglie del sistema punitivo, appare legittimato da considerazioni di politica criminale: poiché esse, per la loro struttura e per la rilevanza dei danni che determinano, sono assimilabili ad altre fattispecie integranti i reati di furto o di truffa, talché, se potesse ricorrersi al ragionamento analogico nel diritto penale, se ne giustificerebbe la loro attuale punibilità.

Si profila, pertanto, l'opportunità di introdurre un'autonoma previsione di reato per le frodi informatiche, come di recente è avvenuto nella Germania Federale, con la seconda legge contro la criminalità economica (2 WIKG, 15 maggio 1986)²⁵⁵.

V. TUTELA DELL'ELABORATORE

1. *Il reato di danneggiamento negli Stati Uniti.*

Nel diritto statunitense, come negli altri ordinamenti, non sono state poste particolari questioni di qualificazione giuridico-penale in relazione alle ipotesi di asportazione o di danneggiamento dolosi dell'elaboratore (o delle sue singole componenti fisiche o dei dispositivi ad esso eventualmente collegati) configurando tali attività lesive i reati di furto o di danneggiamento comuni²⁵⁶.

²⁵⁵ Ragioni analoghe a quelle che hanno fatto ritenere non punibili diverse ipotesi di frodi informatiche nell'ordinamento italiano, si erano proposte anche in relazione al diritto tedesco occidentale, sul punto cfr. K. TIEDEMANN, *op. cit.*, p. 620; W. HARTMANN, *op. cit.*, p. 14. Al riguardo il progetto di legge in appendice alle opere di K. TIEDEMANN, *cit.*, p. 63 e C. SARZANA, *Note, cit.*, p. 25. Con la 2WIKG, infine, si è introdotto l'art. 263a (truffa mediante computer). Non sembrerebbe aver posto altrettante difficoltà la perseguibilità del fatto nell'ordinamento francese. Non si è esclusa la configurabilità del reato di *escroquerie* (art. 405 code pén.) applicando un orientamento giurisprudenziale in tema di distributori automatici che rifiutava di considerare la macchina come destinatario delle false informazioni ed imponeva di « *chercher l'homme derrière la machine* ». Né si è rite-

nuto di limitare la configurabilità del reato ai soli casi di consegna materiale, escludendo così tutte le ipotesi in cui l'elaboratore attua accreditamenti, applicando la giurisprudenza in tema di frodi fiscali. (Così P. SARGOS e M. MASSE, *op. cit.*, p. 29; J. PRADEL e C. FEUILLARD, *op. cit.*, p. 310; R. GASSIN, *op. cit.*, p. 39). Analoghe considerazioni vengono svolte in Belgio: v. J. SPREUTELS, *op. cit.*, p. 366 inoltre, A. MANNA, *op. cit.*, p. 506.

Anche in Gran Bretagna non pare che la perseguibilità del fatto abbia sollevato problemi, al riguardo L. MENNELLY, *op. cit.*, p. 599. Per un'analisi comparata della normativa e delle riforme internazionali in tema di truffa, cfr. U. SIEBER, *The International, cit.*, p. 39 s.

²⁵⁶ Cfr. U.S. DEPARTMENT OF JUSTICE, *Legislative resource, cit.*, p. 3.

Il mero intento di aggravare le pene edittali applicabili ha perciò condotto alcuni Stati americani ad inserire nel contesto delle leggi sulla criminalità informatica, l'espressa previsione del danneggiamento dell'elaboratore o delle sue componenti. Secondo la tecnica legislativa adottata rispetto ad altre ipotesi delittuose, anche il danneggiamento dell'elaboratore è previsto sia come condotta integrante un'autonoma fattispecie di reato²⁵⁷, ma talora anche come elemento costitutivo d'una fattispecie complessa, caratterizzata dall'intento di commettere (o progettare) una frode o comunque di ottenere proprietà o servizi²⁵⁸.

Per analoghe ragioni è stato presentato al Congresso Federale un progetto di legge per l'introduzione d'una norma incriminatrice, per contenuto e struttura, analoga a quelle statali dianzi indicate²⁵⁹.

La norma, una volta approvata, verrebbe a concernere il danneggiamento doloso di elaboratori (o loro componenti) che operano nell'ambito del commercio interstatale, per enti finanziari, per il Governo Federale od uffici governativi, che le leggi statali non potevano sanzionare data la ripartizione costituzionale delle competenze.

Interessa rilevare che ove l'introduzione della previsione del danneggiamento di elaboratore sia associata ad una definizione legislativa del termine *computer* troppo vasta, la normativa introdotta verrebbe a sanzionare anche ipotesi di modesto rilievo, come i danni dolosamente provocati a macchine da scrivere, od orologi al digitale, senza che la gravità o la specificità del fatto giustifichino l'applicazione delle pene normalmente più severe previste per il reato speciale.

²⁵⁷ « *A person commits computer fraud (om.) by intentionally and without authorization damaging or destroying any computer system or computer network* ». Ariz. Rev. Stat. Anno. par. 1323-16B; con diverse formulazioni: Cal. pen. Code, par. 502c; Colo. Rev. Stat. 18-5.5-102 (2); Mich. Stat. Ann., par. 28.529 (5); N.M. Stat. ann. 30-16A-4; N.C. Gen. Stat. par. 14-455 (a); R.I. Gen. Laws 11-52-3; Ga Code Ann. par. 16-9-93 (b); Connecticut Act of May 31, 1984, par. 2 (f); Idaho Code, 18-2202 (2) Iowa Act of May 10, 1984, par. 5; Louisiana, Act of July 13, 1984; Minn. Stat. Ann., 609.88 (1) (a); MO Ann. Stat. 569.097; Nev. Rev. Stat. 205.476; N.D. Cent. Code 12.1-06.1-08 (2); Oklahoma Computer Crimes Act, Ch. 70 par. 3; 18 Pa Cons. Stat. Ann. par. 3933; Tenn. Code Ann. par. 39-3-1404 (b); Wyo Stat. 6-3-503. Fla. Stat. Ann. 815.05 (2) (a), quest'ultima norma prevede un'aggravante ove il danneggiamento dell'elaboratore o di sue parti comporti l'interruzione di servizi pubblici.

²⁵⁸ « *A person commits computer fraud...*

by ...damaging, destroying without authorization any computer, computer system computer network or any part of such computer, system or network with the intent to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false and fraudulent pretenses, representations or premises ». Ariz. Rev. Stat. Ann. 13-2316A; e analogamente: Cal. pen. code par. 502 b; Ill. crim. code 16-9 (b) 3; Iowa Act cit., par. 6. SDLaws Ann. 43-43B-1 (2).

²⁵⁹ Nel progetto S. 240 (del 1979) è contenuto il par. 1028 (b), che prevede: « *Whoever intentionally and without authorization, directly or indirectly, ... alters, damages, or destroys or attempts to damage or destroy any computer, computer system or computer network described in sec. (a)* ». Il progetto S. 240 del 1980 prevede esclusivamente il danneggiamento ed esclude l'alterazione. Entrambi i progetti concernono, come si è già precisato gli elaboratori che operano nel commercio interstatale od appartengono, od operano per il Governo, enti od organi pubblici, o sono interconnessi a computer pubblici.

2. *Fattispecie configurabili in Italia.*

Esaminando la legislazione italiana in materia, si può rilevare che il danneggiamento doloso degli elaboratori è in astratto riconducibile a due fattispecie distinte di reato: il danneggiamento comune previsto dall'art. 635 cod. pen. e l'ipotesi di attentato agli impianti di elaborazione descritta dall'art. 420 cod. pen. introdotto dalla legge n. 59 del 1978²⁶⁰. Questa disposizione presenta particolare interesse, perché, insieme all'art. 623-bis cod. pen., è una delle scarse fattispecie che specificamente concernono la nuova tecnologia informatica.

Non è fuor di luogo però considerare che l'espressa previsione dell'attentato agli impianti di elaborazione non è intervenuta allo scopo di sanare alcuna lacuna presente nell'ordinamento (poiché i fatti lesivi in essa previsti potevano esser ricondotti senza alcuna difficoltà nell'ambito del reato di danneggiamento comune). È piuttosto allo scopo di aggravare le pene per i fatti in essa descritti, in ragione della ritenuta maggior gravità dei medesimi, che la norma è stata inserita nel codice penale²⁶¹.

Il rilievo che le norme degli artt. 420 e 635 cod. pen. presentano aree di coincidenza rende opportuno tentare di individuare i fattori che presiedono alla specializzazione dell'una rispetto all'altra.

Un primo dato di specificità contenuto nell'art. 420 può esser individuato nella tassativa previsione dell'oggetto materiale del reato: impianti di elaborazione di dati e di pubblica utilità, cui per contro corrisponde la generica dizione « cose » contenuta nell'art. 635 cod. pen. Va, al riguardo, precisato che nell'espressione « impianti di elaborazione » non possono ritenersi compresi tutti gli elaboratori: le due nozioni tecniche, infatti, non coincidono, rappresentando l'elaboratore una mera componente degli impianti di elaborazione dei dati, che usualmente sono strutturati in un'unità centrale ed in diverse unità periferiche ad essa collegate.

Per tale ragione la tassativa previsione dell'art. 420 non dovrebbe esser applicabile al danneggiamento di un terminale o di un elaboratore privo di collegamenti con unità periferiche, che dovrebbero esser invece ricondotti nell'ambito della fattispecie dell'art. 635.

Il secondo dato di specificità riguarda la particolare struttura del reato previsto dall'art. 420, la cui consumazione è anticipata al livello del mero attentato. Mentre il reato di danneggiamento comune si consuma esclusivamente con l'effettiva lesione dell'integrità o

²⁶⁰ Sulla legge v. A. DALIA, *L'attentato agli impianti ed il delitto di riciclaggio*, Milano, 1979; C. PALAZZO, *La recente legislazione penale*, Padova, 1985, p. 141 e, quanto alla

specifica ipotesi di sabotaggio informatico: C. RAPISARDA, *op. cit.*; L. PICOTTI, *La rilevanza penale*, cit.

²⁶¹ Cfr. A. DALIA, *op. cit.*, p. 18 ss.

della funzionalità della cosa; per la perfezione dell'ipotesi speciale è, invece, sufficiente che sia insorto il pericolo di danno²⁶².

Un efficace correttivo alla scarsa tipizzazione della condotta punibile, propria della fattispecie di attentato in genere (e di questa in particolare) è rinvenuto dalla più recente dottrina e dalla giurisprudenza della necessaria considerazione, ai fini della configurabilità del reato, dell'idoneità dell'azione ad esporre a pericolo il bene tutelato dalla norma²⁶³.

In base a tali considerazioni un preminente ed ulteriore dato di specificità della disposizione speciale può dunque esser ravvisato nel ruolo determinante per l'integrazione del reato svolto dall'interesse tutelato dall'art. 420 cod. pen.: l'ordine pubblico²⁶⁴. Si dovrebbero, perciò, ricondurre nella fattispecie di attentato ai centri di elaborazione, solo quei fatti che possano comportare un significativo pregiudizio dell'ordine pubblico suscitando turbamento ed apprensione nella collettività²⁶⁵. Ne deriva che il danneggiamento di centri di elaborazione che non sia idoneo a determinare compromissione della pace pubblica, può integrare esclusivamente il reato previsto dall'art. 635 cod. pen. Ad altrimenti ritenere d'altronde non si giustificerebbe l'energica tutela e la severità che il legislatore ha inteso riconnettere alla norma dell'art. 420 cod. pen.

VI. BREVI CONSIDERAZIONI SULLA TECNICA SANZIONATORIA ADOTTATA NELLA RECENTE LEGISLAZIONE STATUNITENSE

Esaminate le singole fattispecie di reato introdotte nell'ambito della recente legislazione sui *computer crimes*, seppur in linee solo generali, appare opportuno integrare le considerazioni svolte, con qual-

²⁶² V. A. DALIA, *op. cit.*, p. 34; per un compiuto inquadramento della fattispecie, sotto il profilo della descrizione normativa della condotta, cfr. E. GALLO, *Il delitto di attentato nella teoria generale del reato*, Milano, 1965; F. BRICOLA, *Teoria generale del reato*, in *Noviss. Dig.*, Torino, 1973, vol. IX, p. 85. L. PICOTTI, *op. ult. cit.*, p. 970 rileva che le norme in esame si diversificano anche in quanto l'art. 420 cod. pen. riguarda esclusivamente il danneggiamento e la distruzione e non le altre condotte tipiche previste dall'art. 635 cod. pen. Si potrebbe al riguardo obiettare che l'art. 420, prevedendo l'attività di « danneggiare » ha effettuato un sintetico richiamo alle condotte di cui all'art. 635 cod.

pen., si dovrebbe così ritenere che il delitto di attentato può sostanziarsi anche nel render inservibile l'impianto.

²⁶³ A. DALIA, *op. cit.*, p. 39 ss.

²⁶⁴ F. MANTOVANI, *Danneggiamento*, cit., p. 112, sottolinea come la *ratio* della diversità d'incriminazione per fattispecie che restano sostanzialmente identiche, va ricercata nella natura del bene giuridico prevalentemente leso o messo in pericolo.

²⁶⁵ Sulla nozione di ordine pubblico valida per la specifica categoria dei reati, e la sua identificazione con il concetto di *ordre dans la rue*, v. C. FIORE, *Ordine pubblico (dir. pen.)*, in *Enc. dir.*, vol. XXX, Milano, 1980, p. 1084; F. ANTOLISEI, *Manuale*, cit., p. 703.

che breve osservazione in merito alla tecnica sanzionatoria applicata dai legislatori statunitensi, con specifico riguardo all'aspetto quantitativo e qualitativo delle pene edittali previste.

Il primo rilievo al riguardo deriva dal raffronto fra le pene irrogabili in base alle nuove leggi e quelle che avrebbero potuto esser inflitte per i fatti previsti anche dalle norme comuni. Si può a proposito riscontrare l'esigenza d'un orientamento legislativo, seppur solo tendenziale, all'aggravamento delle pene per le nuove figure di reato. La maggior severità connessa alle manifestazioni della criminalità informatica trova spiegazione nel preambolo di alcune leggi statali e del progetto di legge federale²⁶⁶. In tali dichiarazioni d'intenti viene attribuita determinante influenza, per l'introduzione delle più gravi norme speciali, sia alla vulnerabilità dei beni connessi ai processi di elaborazione, come alla gravità dei danni usualmente conseguenti ai *computer crimes*, che vengono considerati superiori a quelli normalmente afferenti altre forme di *white-collar crimes*.

È per le medesime ragioni che a livello federale sono state aggravate le pene previste per le ipotesi di spionaggio informatico, rispetto a quelle irrogabili per lo spionaggio comune, mentre la pena prevista per il reato di *wire fraud* (pena detentiva fino a 5 anni congiunta od alternativa ad una pena pecuniaria)²⁶⁷ risulta addirittura triplicata nei progetti di legge volti ad introdurre il reato di *computer fraud* (pena detentiva fino a 15 anni alternativa o congiunta ad una pena pecuniaria)²⁶⁸.

A livello federale si manifesta perciò una tendenza al considerevole aggravamento delle pene edittali in materia di criminalità informatica, per quanto venga assegnato 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.

L'analisi della legislazione statale consente di effettuare ulteriori rilievi in merito alla tecnica sanzionatoria adottata, relativi alla diversa qualificazione del fatto come *felony* o come *misdemeanor* (fra i due concetti v'è approssimativamente lo stesso rapporto che nell'ordinamento italiano insiste fra il concetto di delitto e quello di contravvenzione)²⁶⁹ ovvero alla quantità della pena. Per tali aspetti le

²⁶⁶ Cfr. *Preamble*, in S. 240, 2 *Computer L.J.*, p. 722; nonché l'introduzione alla legge della Florida (Fla. Stat. Ann. par. 81502) ed al progetto delle Hawaji S. 504 in *Riv. cit.*, p. 745.

²⁶⁷ 18 U.S.C. par. 1341.

²⁶⁸ S. 240, propos. 10 U.S.C. 1028 (a), cit.

²⁶⁹ La distinzione fra le due figure è delineata da M.C. BASSIOUNI, *op. cit.*, pp. 100, 113, il quale, inoltre, considera il differente regime che deriva per la pena e le misure di sicurezza.

norme sui *computer crimes* possono esser ricondotte a due modelli fondamentali, tenendo presente che esse, salvo rare eccezioni, appartengono al tipo della norma a fattispecie composita, in cui sono riunite molteplici previsioni di reato.

In primo luogo, taluni Stati nella gradazione della pena o nella qualificazione del reato hanno fatto riferimento al criterio numerico quantitativo del danno patrimoniale subito dalla parte lesa, aggravando la fattispecie di reato in misura direttamente proporzionale al valore della perdita economica²⁷⁰.

È interessante rilevare che, attraverso l'applicazione di tale criterio, talune fattispecie recuperano in specificità e lesività, sicché, ad esempio, le diverse figure di danneggiamento o di falsificazione dei dati, dianzi indicate come ipotesi spesso scarsamente lesive ed ingiustificatamente sanzionate — in particolare nei casi di dati di pubblico dominio o memorizzati in dispositivi di ridotta capacità — risuntano in concreto punibili solo in quanto dal fatto sia derivato un danno apprezzabile per la parte lesa.

Diversamente accade, invece, sulla base delle tecniche sanzionatorie adottate in altri Stati, che prescindono, nel graduare la pena qualitativamente e quantitativamente, dal riferimento al danno, e si affidano piuttosto al diverso criterio della pericolosità del soggetto dedotta attraverso l'intento in concreto perseguito²⁷¹. In tale evenienza l'ipotesi semplice dei diversi reati di accesso abusivo, danneggiamento, alterazione e distruzione dei dati (dei programmi o dell'elaboratore) è qualificata come *misdemeanor*, mentre la qualifica di *felony*, e le più elevate pene, conseguono alla sussistenza dell'ipotesi complessa, costituita oltre che dalle condotte dianzi indicate anche dallo scopo fraudolento, o genericamente criminoso.

In tal caso l'esistenza di forme di temperamento al possibile ricorso all'azione penale anche per fatti di modesta entità è suggerita da alcune considerazioni svolte in sede di analisi economica del diritto, le quali segnalano come la parte lesa sia disinteressata all'instaurazione (e dunque alla denuncia) del processo per fatti di modesta entità, in quanto i *litigation costs* a suo carico supererebbero il risarcimento che potrebbe ricevere²⁷².

Un diverso ordine di indicazioni concernente l'efficacia della normativa sotto l'aspetto preventivo e repressivo può, inoltre, discendere dalla considerazione della persistenza del fenomeno del c.d. « numero oscuro » dei reati informatici, e cioè che i reati effettivamente denunciati siano una parte minima di quelli effettivamente perpetrati e scoperti²⁷³.

²⁷⁰ Colo Rev. Stat. 18-5.5-102 (3); Fla. Stat. Ann. 815.04.2; Ill. Crim. Code 16-9 (c) (1-4); Mich. Stat. Ann., par. 28-529 (7); N.M. Stat. Ann. 30-16A-3 (A) (1-3; 30-16A-4 (A-C).

²⁷¹ In tal senso: Ariz. Crim. Code, 13-

2316 (B-C); Fla. Stat. Ann., 8 15.04 (4) (a-b); 815.05 (2) (b); 815.06 (2b); N.C. Gen. Stat. par. 14-454 (a); (b); Utah Crim. Code par. 76-6-703 (1-5).

²⁷² R.I. ITRIN, *op. cit.*, p. 409.

²⁷³ V. *supra*, nota 219.

Inizialmente l'insorgenza del fenomeno veniva ricondotta principalmente all'esistenza di lacune legislative che non garantivano sufficientemente la vittima riguardo alla possibile condanna del reo²⁷⁴ e solo secondariamente alla negativa pubblicità che la parte lesa avrebbe subito denunciando oltre che il colpevole anche la dubbia sicurezza dei propri centri di elaborazione.

Tuttavia la creazione di specifiche ipotesi di reati informatici, che garantiscono l'effettiva perseguibilità di tali fatti lesivi, da un lato non pare aver ridotto la consistenza del fenomeno del *numero oscuro*, di cui tuttora si riscontra la permanenza²⁷⁵, dall'altro non pare aver spiegato effetti deterrenti, poiché il numero dei *computer crimes* perpetrati, non risulta conseguentemente ridotto.

Sicché appare tuttora preferito il ricorso a forme di repressione diverse dall'azione penale, in particolare all'applicazione di sanzioni contrattuali come il licenziamento, od addirittura il ricorso a forme premiali come l'avanzamento di carriera, onde coinvolgere il responsabile del fatto che si sia dimostrato particolarmente capace nell'organizzazione imprenditoriale ed acquistarne in tal modo la fedeltà²⁷⁶.

Tali evenienze meritano d'esser oggetto di attenta meditazione ove si proponga l'eventualità di introdurre, anche nell'ordinamento italiano, specifiche ipotesi di reato per sanzionare i fatti lesivi, propri della criminalità informatica.

²⁷⁴ Cfr. J.K. TABER, *op. cit.*, p. 277; A. BEQUAI, *op. cit.*, p. 44.

²⁷⁵ J.T. SOMA, *op. cit.*, p. 269; A.M. WAGNER, *op. cit.*, p. 793.

²⁷⁶ A.M. WAGNER, *op. cit.*, p. 794.