ETTORE GIANNANTONIO

I REATI INFORMATICI

SOMMARIO

BENI INFORMATICI E REATI INFORMATICI

Negli ultimi anni l'elaboratore è stato sempre più spesso oggetto o strumento di attività socialmente illecite, ossia di attività che la coscienza dei più considera disoneste; e ciò in quanto si tratta di attività dirette, in genere, a danneggiare altri ovvero a procurare a se stessi un ingiustificato profitto. Ad esempio, sono stati danneggiati impianti elettronici; sono stati danneggiati o falsificati dati o programmi per elaboratore; sono stati compiuti accessi non autorizzati alle memorie ovvero sono state utilizzate abusivamente le unità centrali di un elaboratore; sono stati indotti in errore sistemi di trasferimenti elettronici di fondi in modo da ottenere l'ingiustificato accreditamento di una somma di danaro.

Il fenomeno ha avuto origine negli Stati Uniti d'America, si è diffuso in tutto il mondo ed è normalmente indicato con l'espressione *computer crimes*[1]. Questi costituiscono, ormai, uno dei fenomeni criminali più importanti e tipici del nostro tempo[2] e ad esso sono stati dedicati numerosi studi sia di carattere informatico sia di carattere sociologico[3].

In particolare sono state individuate alcune tecniche illecite tipiche e abituali alle quali sono stati dati nomi a volte pittoreschi come *data diddling*, *logic bombing*[4], *piggybacking*, *trojan horsing*[5],

[1] *I computer crimes* (o *computer related crimes*) sono stati definiti dalla Commissione degli esperti dell'OECD nella riunione tenuta a Parigi nel maggio 1983 come « any illegal, unethical or unauthorized behaviour involving automatic data processing and/or transmission of data » (ogni condotta antigiuridica, disonesta o non autorizzata concernente l'elaborazione automatica e/o la trasmissione dei dati).

[2] Generalmente si ritiene che l'ammontare economico dei danni provocati dai *computer crimes* sia molto rilevante; e ciò per vari motivi:

a) perché attengono a beni di notevole valore (i sistemi informatici, i programmi e le raccolte di dati) e sopratutto per la grande quantità di ricchezza trasferita ogni giorno elettronicamente;

b) per la facilità con cui a volte è possibile penetrare nei sistemi elettronici, sia per la mancanza di osservanza delle norme di sicurezza (c.d. *computer security*), sia per l'ingegnosità di coloro che commettono i computer crimes, a volte al solo scopo di provare la propria abilità (c.d. *hackers*);

c) per il notevole grado di impunità assicurato dalle incertezze della dottrina e della giurisprudenza, dalle difficoltà di accertamento e di prova dei reati, dalla mancanza in molti Stati di attrezzature e di corpi speciali di polizia giudiziaria, dalla ritrosia delle vittime, in specie delle banche, a denunziare i reati subiti (c.d. *dark figure*).

Non è facile, quindi, stabilire con precisione l'ammontare di tali danni. Le indagini più attendibili al riguardo sono quelle condotte negli Stati uniti dallo Stanford Research Institute International a Menlo Park in California, dal General Accounting Office, dal National Center for Computer Crime Data, dall'American Institute of Certified Public Accountants e dall'American Bar Association; in Germania dall'Istituto di criminologia e di diritto penale dell'università di Friburgo, dal Max-Planck Institute per il diritto penale straniero e internazionale di Friburgo, dall'università di Tubinga e dal Bundeskriminalamt.

[3] Sui *computer crimes* o reati informatici esiste ormai un'ampia letteratura.

[4] *Data diddling* sono i casi in cui si sostituiscono dati contenuti nelle memorie di un elaboratore con dati diversi.

Logic bombing sono particolari programmi nascosti che entrano in funzione al verificarsi di certe condizioni alterando o distruggendo i dati o i programmi di un sistema. Questa tecnica è utilizzata normalmente dalle case produttrici di programmi nei casi in cui si verifichi un tentativo di utilizzare un determinato programma da parte di un soggetto non autorizzato. Molte volte, peraltro, la stessa tecnica è utilizzata anche per danneggiare o falsificare sistemi o programmi oppure per distruggere le tracce di un illecito uso dell'elaboratore.

Data diddling e *logic bombing* sono casi tipici di danneggiamento e, a volte, di falsificazione di dati. Un particolare tipo di *logic bombing* sono i cosiddetti *virus*.

[5] *Piggy backing* sono i casi in cui qualcuno si inserisce abusivamente in una linea di comunicazione tra elaboratore e terminale utilizzando indebitamente il codice di utenza di un legittimo e ignaro utente.

Trojan horsing sono tutti i casi in cui un utente riesce ad ottenere informazioni non autorizzate.

Altri casi di accessi abusivi tipici sono detti *wiretapping*, *phone-freak*, *between the lines-entry*, *electromagnetic pickup*, *trap doors*, *data leakage*.

Un programma spesso utilizzato per accessi abusivi è *superzapping*, originariamente creato dalla IBM per superare il controllo delle istruzioni di protezione nel caso di un guasto del sistema.

Gli accessi abusivi molte volte sono effettuati senza alcun fine di lucro, ma al solo scopo di provare la propria abilità informatica da parte dei cosiddetti *hackers*. Spesso si tratta di giovanissimi tanto che in materia di informatica si è parlato, oltre che di criminalità dei colletti bianchi, anche di criminalità in calzoncini corti.

salami technique[6].

Tutte queste fattispecie, e le numerose altre che la fantasia e l'ingegnosità della criminalità informatica continuamente creano, sono a volte di tale gravità economica e sociale da far ritenere giusta e necessaria una sanzione penale.

Non è, tuttavia, facile stabilire se e quando l'attività informatica illecita rientri, in mancanza di una specifica norma incriminatrice, nelle fattispecie previste dalle norme penali vigenti.

Le maggiori difficoltà derivano sopratutto dalla mancanza di accordo sulla natura giuridica dei beni oggetto dei reati informatici. In particolare è controverso se il documento elettronico abbia valore di documento giuridico e, ricorrendone gli estremi, possa essere oggetto dei reati di falso; è controverso se i dati o i programmi possano essere considerati come cose materiali suscettibili di danneggiamento o di furto; è controverso se l'elaboratore possa essere considerato soggetto passivo del reato di furto o di truffa; è, infine, controversa la natura dei programmi per elaboratore e, cioè, se possano essere considerati opere dell'ingegno o invenzioni suscettibili di tutela secondo le norme penali in materia di proprietà dei beni immateriali[7].

Le incertezze della dottrina circa la natura giuridica dei beni informatici in genere e il principio di stretta legalità della norma penale[8] con il correlato divieto del ricorso all'analogia (art. 14 delle disposizioni preliminari al codice civile) hanno indotto gran parte degli autori e della giurisprudenza ad escludere l'applicabilità delle norme comuni di diritto penale in materia di informatica.

Si è così reso necessario un intervento del legislatore che qualificando espressamente come reati alcune forme di abusi informatici ha

[6] *Salami technique* sono i casi in cui piccole somme di danaro (le cosiddette cifre di arrotondamento) vengono distratte dai conti correnti bancari e accreditate indebitamente in un altro conto, creato appositamente. A questo fine vengono utilizzati particolari programmi al posto di quelli previsti per gli arrotondamenti (c.d. *rounding-off utility*).

Salami technique è una delle numerose forme di « truffa » correlate con i trasferimenti elettronici di fondi.

[7] Gli argomenti principali di coloro che escludono l'applicabilità delle norme comuni di diritto penale alle nuove figure di illeciti informatici sono che i beni informatici non hanno una materialità intesa in senso tradizionale; e che l'elaboratore, essendo una macchina e non una persona, non può essere considerato soggetto passivo di reato.

[8] Il principio, già formulato nel diritto romano con l'espressione *nullum crimen, nulla poena sine lege* è codificato in tutti i paesi dell'Europa occidentale (art. 1 cod. pen. italiano, art. 4 cod. pen. francese, art. 103, comma 2 della Costituzione della Repubblica federale di Germania).

posto — o ha tentato di porre — fine alle controversie della dottrina e alle incertezze della giurisprudenza e ha soddisfatto una esigenza punitiva sempre più sentita dalla società nei confronti delle nuove forme di criminalità[9]; e per indicare il complesso di tali norme e dei correlativi problemi interpretativi e applicativi è stato da qualcuno usata, forse un poco affrettatamente, l'impegnativa espressione di diritto penale dell'informatica[10].

È ancora presto per potere dire se il diritto penale dell'informatica avrà un semplice valore descrittivo ovvero acquisterà dignità scientifica e costituirà un nuovo ramo del diritto penale. Va tuttavia osservato che i *computer crimes* o reati informatici non possono comprendere tutti i casi in cui una condotta penalmente sanzionata sia stata posta in essere attraverso l'uso dell'elaboratore, ma dovrebbero essere limitati a quei soli casi in cui oggetto della condotta criminosa sono l'elaboratore e gli altri beni informatici come i dati o i programmi per elaboratori[11]; a quei soli casi, cioè, in cui la particolare natura dei beni informatici pone problemi di applicazione delle vecchie norme e l'esigenza di nuove ipotesi criminose[12].

Questo studio vuole essere un tentativo di ricognizione e di esposizione dei principali problemi in materia di reati informatici, così delimitati.

[9] Le norme più importanti che prevedono i reati informatici in materia economica o di falso sono nel Regno Unito il Forgery and Counterfeiting Act 1981, negli Stati uniti d'America il Federal Counterfeit Access Device and Computer Fraud and Abuse Act 1984 e il Federal Credit Card Fraud Act 1984; in Canada il Criminal Law Amendment Act 1985, in Danimarca la legge 6 giugno 1985, in Germania la seconda legge per la prevenzione dei reati economici 1986, in Francia la loi n. 88-19 relative à la fraude informatique.

Disposizioni in tema di reati informatici sono contenute nelle norme in tema di tutela dei dati personali e di tutela dei programmi per elaboratori. Per le prime vedi l'ampia raccolta contenuta nel volume *Banche dati e tutela della persona*, Camera dei deputati, 2ª ed., Roma, 1983; per le seconde vedi l'opera di V. ZENO-ZENCOVICH, *Le leggi sulla tutela dei programmi per elaboratore in Italia e nel mondo*, Cedam, Padova, 1990.

[10] In particolare il diritto penale dell'informatica è stato definito come « quel gruppo di norme giuridiche con le quali lo Stato proibisce, mediante la minaccia di una pena, determinati specifici comportamenti umani nel campo dell'informatica ». C. SARZANA, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1984, I, p. 22 ss.

[11] Infatti se si ritenesse che il diritto penale dell informatica comprenda tutte le ipotesi in cui un'attività criminosa è stata posta in essere a mezzo dell'elaboratore, esso finirebbe, a causa dell'invadenza dell'elaboratore in ogni campo dell'attività umana, per comprendere la maggior parte delle ipotesi criminose. È stato al riguardo paradossalmente affermato che un computer può anche uccidere ed è stato citato, a comprova, il pietoso caso del suicidio di un agente di borsa a causa di una falsa informazione dell'elaboratore sulla propria situazione economica o altre ipotesi di carattere fantascientifico come quella dei cosidetti messaggi subliminali.

[12] La originalità del diritto dell'informatica è fondata proprio sull'originalità del bene informatico, un nuovo tipo di bene che presenta caratteristiche proprie diverse sia da quelle dei beni materiali, sia da quelle dei beni immateriali tradizionalmente riconosciuti nel campo giuridico.

In particolare saranno esaminate le seguenti fattispecie:

a) Casi in cui oggetto della condotta criminosa è l'elaboratore inteso nella sua materialità ovvero nella sua funzionalità. Questi casi sono regolati dalla legge 18 maggio 1978, n. 191 che ha nuovamente introdotto nel codice penale il già abrogato art. 420 e punisce espressamente con sanzioni particolarmente severe il danneggiamento di impianti di elaborazione dei dati. Si tratta di una delle poche norme emanate in materia dal legislatore italiano e non presenta particolari problemi applicativi quando l'attentato riguarda l'elaboratore nella sua materialità, il cosidetto *hardware*. La norma è stata, peraltro, applicata da alcune decisioni giurisprudenziali anche nei casi di danneggiamento dei dati e dei programmi quando il danneggiamento sia di tale rilevanza da incidere sulla funzionalità stessa dell'elaboratore (vedi § 3, §§ 1).

b) Casi in cui oggetto della condotta criminosa sono i documenti elettronici, ossia i dati o i programmi per elaboratore in qualche modo memorizzati, sia pure in forma digitale. In tali casi si discute se il documento elettronico abbia valore di documento giuridico e possa quindi essere oggetto dei reati di falso ovvero di furto o di danneggiamento di documenti (vedi § 1, § 2, § 3).

c) Casi in cui la condotta criminosa ha per oggetto l'accesso o l'utilizzazione abusiva di un elaboratore. Sono i casi in cui la legislazione americana parla di *unauthorized access e di computer abuse*. Nella nostra legislazione non vi sono norme in materia e non riusciti sembrano i tentativi di configurare le fattispecie in questione come furto d'uso o furto di informazioni, violazione di domicilio o sostituzione di persona; e numerose difficoltà sorgono anche per la configurabilità del reato di intercettazione delle comunicazioni telefoniche e telegrafiche prevista dall'art. 632-*bis* cod. pen. (vedi § 4).

d) Casi in cui oggetto della condotta criminosa è l'esatto funzionamento di un sistema elettronico, in specie di un sistema di trasferimenti elettronici di fondi, che viene alterato dal reo per procurarsi un ingiusto profitto. Sono i casi previsti espressamente dalle leggi statunitensi come *computer fraud*; in Italia, ad eccezione della recente norma prevista dall'art. 12 della legge 197/1991, non vi sono norme che prevedano la fattispecie e si nega in dottrina e in giurisprudenza che sussistano gli estremi della induzione in errore di una persona richiesti per il reato di truffa (vedi § 6).

e) Casi in cui la condotta criminosa ha per oggetto la violazione delle norme a tutela dei dati personali, di quelle norme, cioè, che limitano la possibilità di raccolta dei dati personali o attribuiscono all'individuo il potere di controllare le raccolte contenenti i propri dati personali.

In Italia, in mancanza di una norma in materia, le uniche disposizioni che regolano le banche dei dati personali sono contenute nella legge 121/1981 istitutiva del centro di elaborazione dati presso il Ministero dell'interno (vedi § 6).

1. Il falso informatico.

1.1. *I reati di falso e la nozione di documento.*

Come è noto, nel nostro ordinamento i reati di falso sono previsti nel titolo VII del codice penale, relativo ai delitti contro la fede pubblica, in un apposito capo, il capo III, denominato « della falsità in atti » e costituito dagli artt. da 476 a 493.

La materia, è stato osservato, è diluita in una minuta e non sempre completa statistica con una esasperante serie di distinzioni e sotto distinzioni[13]; l'oggetto, peraltro, è unico ed è costituito dalla tutela della pubblica fede insita in ogni documento[14]; e ciò sia nei confronti di chi sopprima o alteri un documento vero, sia nei confronti di chi formi un documento falso.

La nozione del documento quale bene giuridico a se stante e oggetto materiale dei reati di falso ha, dunque, fondamentale importanza nella materia del falso documentale; e, infatti, fino a quando si considerò il documento solo come uno dei vari mezzi di prova, la falsità in atti non assunse una configurazione autonoma, ma venne confusa con la falsità degli altri mezzi di prova oppure con i reati di frode e di truffa[15].

La nozione di documento, tuttavia, è oggetto di una antica e ancor viva controversia che si polarizza intorno a due opinioni: una, più ampia, « fondata sulla necessità di dare una definizione valida per tutto l'ordinamento giuridico, avulsa così dal mezzo della sua formazione »; l'altra, più ristretta, « nascente dagli scopi peculiari della protezione penale di determinati atti e perciò legata al mezzo che nella legge penale viene in considerazione »[16].

[13] Antolisei, *Manuale di diritto penale*, vol. 2, p. 477, Giuffrè, Milano, 2ª ed., 1956. Dello stesso Autore vedi anche l'articolo *Nebuloso frammentarismo in materia di falso*, in *Giur. it.*, 1950, II, p. 57.

[14] La nozione di pubblica fede risale al Genovesi e consentì al Filangieri e, quindi, a tutti i codici moderni di formulare la classe dei reati contro la fede pubblica e di comprendere in essa i delitti di falso documentale. Sulla nozione di pubblica fede v. Ebner - Romano di Falco, *Fede pubblica (Delitti contro)*, in *Noviss. Dig. it.*, vol. V, p. 1072, Utet, Torino, 1938; Cristiani, *Fede pubblica (Delitti contro)*, in Noviss. Dig. it., vol. VII, p. 173, Utet, Torino, 1961; Malinverni, *Fede pubblica (dir. pen.)*, in *Enc. dir.*, vol. VII, p. 69, Giuffrè, Milano, 1968.

[15] Sulla storia dei reati di falsità e di falso v. Ferrini, *Falso (materia penale: diritto romano)*, in *Dig. it.*, vol. XI, p. 218, F.lli Bomba, Torino, 1895; Brasiello, voce *Falsum*, in *Noviss. Dig. it.*, vol. VII, p. 33, Utet, Torino, 1961; Scarlata Fazio, voce *Falsità e falso (storia)* in *Enc. dir.*, vol. XVI, p. 504, Giuffrè, Milano, 1967.

[16] De Marsico, *Falsità in atti*, in *Enc. dir.*, vol. XVI, p. 570, Giuffrè, Milano, 1967.

Una definizione in senso ampio di documento è quella famosa di Carnelutti per il quale il documento (da docere, insegnare) è una cosa che ci fa conoscere un fatto e si contrappone al testimone che è una persona che narra e non una cosa che rappresenta[17].

Altre definizioni in senso ampio sono quella del Malinverni che, rifacendosi al Mommsen (« documento è un pensiero passato di durevole riconoscibilità »), definisce il documento come « l'oggetto che rappresenta un pensiero »[18]; e quella del Guidi che, parafrasando lo Schultze, definisce il documento come « un oggetto corporale, prodotto dall'umana attività di cui conservi le tracce il quale, attraverso la percezione dei grafici sopra di esso impressi, o delle luci o suoni che può fornire, è capace di rappresentare, in modo permanente, a chi lo ricerchi, un fatto che è fuori di esso documento »[19].

Tradizionale e ancora prevalente nel diritto penale è la nozione più ristretta che identifica il documento con i soli documenti scritti. Una definizione particolarmente autorevole è quella del Manzini per il quale il documento è « ogni scrittura fissata sopra un mezzo trasmissibile, dovuta ad un autore determinato, contenente manifestazioni o dichiarazioni di volontà ovvero attestazioni di verità, atte a fondare o a suffragare una pretesa giuridica o a provare un fatto giuridicamente rilevante in un rapporto processuale o in un altro rapporto giuridico »[20].

Lo stesso Autore osserva, a sostegno della essenzialità della forma scritta, che « nel documento la fuggevole, inafferrabile manifestazione del pensiero viene raccolta, trattenuta e tramandata materialmente col mezzo della scrittura che spiritualizza la materia e materializza il pensiero si che la materia scritta e l'espressione ideale si immedesimano in una entità concreta, unitaria e inscindibile... il muto linguaggio del documento continua a disporre o ad attestare anche quando la voce del disponente o dell'attestante è spenta per sempre ovvero quando contrari interessi o propositi illegittimi pretendano disconoscere o modificare quanto è già stato disposto... »[21].

In sostanza il legislatore penale ha, più o meno consapevolmente, seguito la nozione ristretta di documento e tutte le ipotesi previste di falso documentale presuppongono quantomeno un documento scritto. La nozione più ampia di documento, accolta con utili risultati in

[17] CARNELUTTI, *Teoria del falso*, Cedam, Padova, 1935 p. 139.

[18] MALINVERNI, *Teoria del falso documentale*, Giuffrè, Milano, 1985, p. 15.

[19] GUIDI, *Teoria giuridica del documento*, Giuffrè, Milano, 1950, p. 46.

[20] MANZINI, *Trattato di diritto penale*, vol. VI, p. 555, n. 2218, Utet, Torino, 1935.

[21] MANZINI, *Trattato di diritto penale*, vol. VI, p. 552, n. 2217, Utet, Torino, 1935.

altri campi del diritto, è sembrata, quindi, alla maggior parte dei penalisti ridondante e fuorviante[22].

Ne consegue che per il nostro ordinamento il documento elettronico in tanto può essere tutelato penalmente in quanto ad esso possa essere riconosciuta la natura di documento scritto.

1.2. *Il documento elettronico come documento scritto.*

I documenti elettronici si possono distinguere in due classi: i documenti elettronici in senso stretto e i documenti elettronici in senso ampio o documenti informatici[23].

I primi sono memorizzati in forma digitale nella memoria centrale ovvero nelle memorie di massa dell'elaboratore e non possono essere letti o comunque percepiti dall'uomo se non a seguito dell 'intervento di apposite macchine traduttrici che rendono percepibili e comprensibili i segnali digitali dai quali sono costituiti.

I documenti informatici o documenti elettronici in senso ampio sono, invece, tutti quei documenti formati dall'elaboratore mediante i propri organi di uscita. Tali documenti non sono necessariamente in forma digitale, ma possono essere costituiti da un testo alfanumerico, un disegno o un grafico memorizzati su un supporto cartaceo, una scheda o un nastro perforato, un microfilm o, comunque, un qualsiasi oggetto materiale formato da una macchina collegata con un elaboratore, come, ad esempio, il braccio meccanico di un robot.

In sostanza, dunque, i documenti elettronici in senso stretto sono destinati ad essere letti dall'elaboratore; i documenti elettronici in senso ampio sono formati dall'elaboratore per essere letti o comunque percepiti dall'uomo senza l'intervento di apposite macchine traduttrici.

L'applicabilità della tutela penale ai soli documenti scritti ha indotto alcuni autori ad escludere che i documenti elettronici in senso stretto possano costituire oggetto diretto di protezione ai sensi delle norme di cui al titolo VII cod. pen.[24].

[22] Osserva ad esempio il MANZINI che « per il CARNELUTTI (*Teoria del falso*, p. 139) per documento si intende qualunque cosa idonea alla rappresentazione di un fatto. Anche ammesso che questa nozione rappresenti un progresso, come sembra all'illustre Autore, e non un regresso (in quanto tende a reintegrare ciò che la scienza ha disintegrato) essa evidentemente non è conforme al diritto penale vigente ». (MANZINI, *Trattato di diritto penale*, vol. VI, p. 556, Utet, Torino, 1935).

[23] E. GIANNANTONIO, *Il valore giuridico del documento elettronico*, in *Riv. dir. comm.*, 1986.

[24] LORENZO PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in questa *Rivista*, 1985, p. 952. Nello stesso senso CARLO SARZANA per il quale « l'alterazione e la cancellazione dei dati contenuti nella memoria dell'elaboratore... molto difficilmente... possono ricadere sotto le previsioni della legge penale italiana relativa al falso poché i dati e le informazioni contenute nel *computer* non possono definirsi giuridicamente documenti almeno ai fini della legge penale ». (C. SARZANA, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1984, I, p. 21).

In particolare è stato osservato che un documento per potere essere tutelato penalmente deve presentare tre requisiti essenziali: l'incorporazione, la comunicabilità e la riconoscibilità. In altri termini deve incorporare dichiarazioni o manifestazioni del pensiero di un uomo, deve essere diretto a comunicare tale pensiero ad un altro soggetto e deve risultare provenire da un autore determinato[25]. I documenti informatici in senso stretto, invece, non presentano alcuno dei requisiti indicati: difatti non sono creati da un uomo e non sono destinati ad essere letti da altri uomini, ma sono creati da una macchina e possono essere letti solo da una macchina.

Il documento rilevante ai fini penali sussisterebbe, invece, solo nel caso dei documenti informatici in senso ampio e, cioè, « solo se e quando il prodotto finale dell'elaborazione del linguaggio macchina verrà riprodotto quantomeno in linguaggio leggibile dall'uomo e nella misura in cui esso venga o debba venire o si debba presumere destinato alla circolazione giuridica e controllata da un uomo e da esso per così dire fatto proprio mediante sottoscrizione o in un altro modo inequivoco... »[26].

Peraltro, è stato anche osservato, « ...in tale fase finale la falsificazione sarebbe già esaurita, in contrasto con la ragione giustificatrice dell'incriminazione autonoma dei reati di falso, diretta ad anticipare il momento della consumazione formale rispetto a quello dell'esaurimento o consumazione materiale dell'azione del reo... »[27].

Una parte della dottrina ha tuttavia sostenuto che anche il documento elettronico in senso stretto può essere considerato un documento scritto; e ciò in base ad una nozione di scrittura più ampia di quella tradizionalmente intesa[28].

È vero, infatti, che normalmente la scrittura consiste nella redazione di segni alfabetici o di cifre del sistema decimale a mezzo di una penna su un foglio di carta. Tuttavia la nozione di scrittura è più ampia di quello che è il suo normale modo di estrinsecazione e finisce per comprendere qualunque dichiarazione incorporata in un supporto materiale destinato a durare nel tempo. In altri termini non è ne-

[25] PICOTTI, *op. cit.*, p. 953.
[26] PICOTTI, *op. cit.*, p. 955.
[27] PICOTTI, *op. cit.*, p. 955.
[28] E. GIANNANTONIO, *Il valore giuridico del documento elettronico*, in *Riv. dir. comm.*, 1986, p. 261; R. BORRUSO, *Computer e diritto*, Tomo secondo, *Problemi giuridici dell'informatica*, p. 216 ss., Giuffrè, Milano 1988.

cessario perché si abbia documento scritto che esso sia redatto in linguaggio alfabetico su un foglio di carta, ma è sufficiente che sia redatto in un qualunque sistema convenzionale di dichiarazione su un qualsiasi tipo di supporto materiale durevole.

Il primo requisito di un documento scritto è, pertanto, la dichiarazione, ossia una combinazione di segni convenzionalmente stabiliti per comunicare con qualcuno o comunque per esprimere un determinato pensiero. Da una parte, quindi, non può considerarsi documento scritto una realtà come, ad esempio, una pallottola conficcata in un muro o un'impronta digitale lasciata da un ladro che, pur se idonea a suscitare in noi pensieri o sentimenti, non sia per sua natura una dichiarazione; dall'altra non rileva nè la lingua, nè il sistema convenzionale di segni usati.

Non importa, infatti, che il documento non sia stato redatto in lingua italiana, ma in una lingua straniera, in dialetto, in una lingua morta, in una lingua artificiale o in un codice convenzionale, purché sia possibile comprenderne alla fine il significato; e non importa che il documento sia stato redatto in stampatello, con segni stenografici, in un alfabeto diverso da quello latino o addirittura in una scrittura non alfabetica, ma pittorica o ideografica[29].

Per quanto riguarda l'altro requisito di un documento scritto, la sua incorporazione in una realtà materiale, va invece osservato che, se normalmente la dichiarazione viene incorporata mediante la penna su un foglio di carta, è anche vero che i documenti possono essere scritti con mezzi diversi e su diversi supporti.

Difatti la giurisprudenza ha ritenuto che un atto debba considerarsi redatto in forma scritta anche in ipotesi diverse da quelle tradizionali e precisamente:

[29] In particolare, nei riguardi di quest'ultima va osservato che mentre la scrittura alfabetica riproduce il suono delle parole aventi un determinato contenuto mediante un sistema di segni convenzionali, la scrittura ideografica riproduce l'immagine delle cose e mediante esse il contenuto del pensiero. Entrambe, tuttavia, sono destinate alla comunicazione e, come è stato osservato, « non infrequentemente un documento ha carattere misto, perché è in parte scritto con scrittura alfabetica (ad esempio, contesto di un rogito notarile) ed in parte con scrittura ideografica (ad esempio, numeri, formule, disegni). È necessario, però, che la scrittura ideografica corrisponda ad un sistema di decifrazione e di interpretazione generale e universale, accessibile ugualmente da tutti come nel caso della scrittura per geroglifici egiziani, o per ideogrammi cinesi. Negli altri casi si parla di contrassegni ». (MALINVERNI, *Fede pubblica (dir. pen.)*, in *Enc. dir.*, vol. XVII, p. 87, Giuffrè, Milano, 1968). L' Autore parla in questi casi di contrassegni « che riproducono immagini che richiamano direttamente pensieri, indipendentemente dalla lingua in cui possono essere tradotti » e li distingue dai segni « che non esprimono il pensiero di chi li ha prodotti » e non rientrano quindi nel concetto di documento come, ad esempio, un gettone telefonico.

a) per quanto riguarda la materia anche se non è redatto su carta, ma su una materia diversa, come la pelle o il tessuto o, in genere, ogni altra materia su cui sia possibile imprimere con qualsiasi mezzo idoneo dei segni grafici[30];

b) per quanto riguarda il mezzo anche se non è redatto con la penna, ma con una matita, con il gesso o con il carbone e, qualora non sia richiesta l'autografia, anche con una macchina da scrivere, sia normale sia con caratteri stenografici[31].

È necessario tuttavia che si tratti di una realtà materiale che, pur non essendo necessariamente indistruttibile, presenti tuttavia una certa idoneità a perdurare nel tempo. Non possono, quindi, considerarsi documenti le dichiarazioni scritte sulla neve o sulla sabbia ovvero tracciate in cielo dagli aerei con vapori colorati.

La nozione ampia di scrittura così accolta fa sì che non soltanto il documento elettronico in senso ampio, ma anche il documento elettronico in senso stretto possa essere considerato documento scritto in quanto anch'esso consiste in definitiva di una dichiarazione incorporata su un supporto materiale durevole. Esso, infatti, contiene un messaggio (che può essere un testo alfa-numerico, ma anche un disegno o un grafico), in un linguaggio convenzionale (il linguaggio dei *bit*), su un supporto materiale mobile (in genere nastri o dischi magnetici o memorie circuitali) e destinato a durare nel tempo (sia pure in modi diversi a seconda che si tratti di memoria di massa, di memorie volatili, di memorie *ram* o di memorie *rom*)[32].

È stato obiettato che nel documento elettronico in senso stretto non vi è una rappresentazione materiale in quanto i *bit* che ne costituiscono l'alfabeto sono entità fisiche non percepibili dai sensi umani; e che lo stesso linguaggio elettronico o, meglio, digitale, non è un

[30] È stata pertanto ritenuta scrittura privata la dichiarazione di autenticità di un quadro vergata a pennello a tergo del quadro stesso e firmata dal suo autore (Trib. Roma 31 marzo 1965, in *Foro it.*, 1966, II, 513).

[31] È stato, ad esempio, ritenuto valido il testamento scritto da un condannato a morte con il proprio sangue su un muro della prigione.

[32] I documenti elettronici in senso stretto possono avere un diverso grado di conservabilità. Alcuni, infatti, come, ad esempio, i dati contenuti nelle memorie circuitali RAM (Random Access Memory) sono di carattere volatile, ossia si cancellano automaticamente appena viene spento l'elaboratore. Altri, invece, come i dati contenuti in nastri o dischi magnetici o ottici e in genere nelle memorie di massa rimangono memorizzati finché un intervento umano non provveda a cancellarli; altri, infine, come i dati contenuti nelle memorie ROM (Read Only Memory) sono destinati a permanere inalterabili nel tempo.

vero e proprio linguaggio, ossia un mezzo di comunicazione, perché non è destinato a comunicare qualcosa ad altri esseri umani, ma solo a far funzionare una macchina.

Entrambe le obiezioni sembrano tuttavia infondate. I *bit* della scrittura digitale sono entità fisiche, magnetiche o circuitali ad esempio, e quindi realtà materiali anche se non percepibili con i sensi umani[32-bis].

Inoltre occorre osservare che in genere il documento non si limita a far funzionare una macchina, ma vuole, attraverso il funzionamento di questa, comunicare nel modo più rapido e efficace possibile, con un più vasto numero di persone; e che qualsiasi documento elettronico può essere compreso da chiunque purché sia stato redatto secondo un codice, anche se segreto, ovvero, se si tratta di programmi, secondo un linguaggio le cui regole permettano di risalire all'intento dell'autore.

Infatti la giurisprudenza ha da tempo affermato che deve considerarsi scritto anche un documento che, redatto a mezzo di matita simpatica, non possa essere letto se non mediante un'apposita macchina e un apposito procedimento; e che, parimenti, deve considerarsi documento scritto un documento redatto in un codice convenzionale, anche se segreto.

La ritenuta natura di documento scritto non comporta per ciò solo l'applicabilità al documento elettronico in senso stretto delle norme in tema di falso documentale. Queste, infatti, non si applicano a tutti i documenti scritti, ma hanno per oggetto quasi esclusivo gli atti pubblici e le scritture private. Occorre, quindi, riconosciuta al documento elettronico, anche se in senso stretto, la natura di documento scritto, accertare se esso possa essere considerato scrittura privata o atto pubblico.

1.3. *Documento elettronico e falsità in scrittura privata.*

Il documento elettronico in senso stretto, anche se può essere considerato documento scritto, non può avere il valore di scrittura privata o di atto pubblico se un'apposita norma non lo preveda espressamente.

Requisito essenziale della scrittura privata, infatti, è la sottoscrizione, cioè l'apposizione del proprio nome e cognome da parte della persona da cui risultano provenire le dichiarazioni che formano il testo della scrittura.

[32-bis] Per un'analisi della nozione di materialità nel diritto vedi più avanti § 2 in tema di furto.

Come è noto, la sottoscrizione ha una triplice funzione: una funzione indicativa in quanto serve a indicare l'autore del documento; una funzione dichiarativa di assunzione della paternità del documento; e una funzione probatoria che permette di accertare se l'autore della sottoscrizione sia effettivamente colui che è stato indicato nella sottoscrizione stessa.

Si presume, in altri termini, che ogni individuo abbia un suo particolare modo di sottoscrizione mai perfettamente riproducibile; e che un'apposita scienza, la scienza grafologica, possa mettere in evidenza e accertare con sicurezza le differenze tra una sottoscrizione autentica e una contraffatta. Di qui la necessità che la sottoscrizione sia autografa, ossia apposta di proprio pugno da parte del sottoscrittore: essa può essere redatta anche con caratteri a stampatello, ma non con mezzi meccanici.

Dobbiamo, quindi, chiaramente distinguere il valore giuridico del documento scritto dal valore della scrittura privata e riconoscere al documento elettronico in senso stretto valore di documento scritto e non di scrittura privata per l'impossibilità dell'atto di sottoscrizione personale.

Nulla vieta, invece, che un documento elettronico in senso ampio, cioè formato con l'ausilio dell'elaboratore, possa costituire una valida scrittura privata. Così, ad esempio, nel caso di un tabulato formato mediante una stampante collegata con il sistema di elaborazione e sottoscritto dalle parti[33].

La configurabilità dei reati di falso in scrittura privata va pertanto limitata a quei soli casi in cui la legge preveda la falsità di documenti normalmente non sottoscritti come i registri e le carte domestiche, i libri di commercio e le fatture (art. 484 cod. pen.)[34].

Non sussistono decisioni giurisprudenziali al riguardo. È, tuttavia, opportuno ricordare alcune sentenze in cui la giurisprudenza ha entro certi limiti considerato le registrazioni digitali equivalenti alle scritture tradizionali. Si tratta delle decisioni in materia di violazione degli obblighi relativi alle scritture contabili per la mancata trasposizione dei dati contabili memorizzati da un supporto magnetico a un supporto cartaceo entro il termine di sessanta giorni di cui all'art. 22 del d.P.R. n. 600/1973.

[33] Tuttavia anche il documento elettronico in senso ampio non può sostituire la scrittura quando per la validità dell'atto è necessaria non soltanto la sottoscrizione, ma anche la formazione autografa dell'intero atto, come nel caso del testamento (art. 602 cod. civ.).

[34] Sulla fattura elettronica vedi l'articolo di L. GRISOSTOMI di prossima pubblicazione nella *Rivista di diritto commerciale*.

In particolare il Tribunale di Parma con sentenza 23 marzo 1988 ha affermato che la mancata trasposizione nel termine stabilito costituisce reato poiché l'immagazzinamento dei dati in memoria non può ritenersi equivalente alla loro trascrizione sui registri contabili[35].

A sostegno il Tribunale ha osservato che « la registrazione su nastri magnetici non ha il carattere della definitività, potendo essere modificata a discrezione dell'operatore e trovando tale provvisorietà limite esclusivo nella stampatura della memoria ».

Di contrario avviso sono state, invece, le decisioni del Tribunale di Firenze 11 marzo 1986, del Tribunale di Lecco 28 luglio 1986, del Tribunale di Viterbo 21 novembre 1986 e dello stesso Tribunale di Parma 22 marzo 1988[36].

In particolare quest'ultima decisione ha osservato che « il problema va affrontato e risolto avendo presente da un lato la ratio del reato de quo che è quella di consentire in ogni circostanza un'agevole verifica fiscale dei redditi e dell'imponibile tributario e dall'altra l'imprescindibile necessità per le imprese di potere utilizzare tutti quei mezzi che la moderna tecnica metta a loro disposizione per fronteggiare la complessa serie di adempimenti di natura contabile e fiscale loro imposti in maniera adeguata e al tempo stesso economicamente conveniente e cioè attraverso una razionale gestione delle apparecchiature »; che « il pubblico ministero d'udienza, nel richiedere la condanna dell'imputato, aveva, fra l'altro, evidenziato che la memorizzazione dei dati contabili su supporti elettromagnetici non esclude una possibile successiva alterazione degli stessi mediante opportune cancellazioni e variazioni di guisa che, non rimanendo traccia alcuna delle originarie registrazioni, la contabilità in tale modo ottenuta non offrirebbe quelle garanzia di sicurezza, che solo la tempestiva trascrizione dei dati nelle prescritte scritture contabili inequivocabilmente assicura »; che « la prospettata tesi, pur muovendo dall'esatto presupposto che la contabilità deve essere tenuta con modalità tali da evitare qualunque possibilità di evasione fiscale e pur formulando l'esatto rilievo che è tecnicamente possibile procedere ad una manipolazione dei dati originariamente inseriti, per cui teoricamente sussiste una possibilità di alterazione o cancellazione degli stessi, trala-

[35] Trib. Parma 23 marzo 1988 (presidente Grassi, estensore Padula, imputato G.M.) in questa *Rivista*, 1989, p. 192 e in *Corr. trib.*, 1988, 2723.

[36] Trib. Viterbo 21 novembre 1986 (presidente Caliendo, estensore Bianchini, imputato P.G.) in questa *Rivista*, 1987, p. 1067 e in *Corr. trib.*, 1987, 918; Trib. Parma 22 marzo 1988 (presidente Mossini, estensore Piscopo, imputato M.F.) in questa *Rivista*, 1989, 192 e in *Corr. trib.*, 1988, 2723. Le sentenze del Tribunale di Firenze e di Lecco sono citate nella motivazione della sentenza del Tribunale di Parma 23 marzo 1988.

scia, tuttavia, di valutare che nel caso di specie sussistono due obiettive condizioni che escludono una siffatta possibilità e cioè:

1) la regolare tenuta del registro elaborazione dei dati dal quale risulta, in relazione al periodo de quo, la tempestiva memorizzazione di tutte le fatture di vendita e di acquisto e di tutti i movimenti contabili effettuati per cassa e tramite banche;

2) la regolare effettuazione della liquidazione trimestrale IVA ».

Il Tribunale ha quindi affermato che « la presenza di siffatte condizioni nonché la stessa tecnica di registrazione sequenziale escludono una concreta possibilità di manipolazione dei dati originariamente inseriti. Ne consegue che non può essere messa in dubbio l'attendibilità delle registrazioni contabili effettuate a mezzo di elaboratori elettronici, anche nel caso che le stesse non siano state ancora definitivamente stampate sui prescritti supporti cartacei previsti dalla normativa fiscale, e ciò sia, peraltro, immediatamente ottenibile in caso di verifica fiscale ».

Secondo il Tribunale, in sostanza, « le registrazioni contabili de quibus, puntualmente e definitivamente memorizzate a mezzo di una macchina elettrocontabile , pur se non pedissequamente trasferite sul prescritto supporto cartaceo fiscale nel prescritto termine di sessanta giorni dalla effettuazione delle singole operazioni, escludono la ravvisabilità del reato p.p. dall'art. 1, comma 2, nn. 1 e 2 legge 7 agosto 1982, n. 516 atteso che in tal caso la mancata stampa del libro giornale non può essere equiparata all'omessa annotazione punita con la menzionata norma »; e che invece si deve « considerare l'indicata memorizzazione, tempestiva e definitiva, valido equipollente alla registrazione sulle pagine del libro-giornale, per cui deve ritenersi che l'adempimento tributario sia stato sostanzialmente soddisfatto ».

A conforto della propria tesi il Tribunale richiama « sia la circolare n. 40-9-4056 del 26 novembre 1981 emanata dalla Direzione generale delle imposte dirette la quale riferendosi alla tenuta della contabilità di magazzino dichiara espressamente che, ai fini delle imposte dirette, il termine di sessanta giorni deve essere inteso come registrazione delle transazioni su supporti fisici riconoscendo la possibilità di stampare il relativo giornale a fine d'anno (il che equivale a dire che, in presenza di sistemi computerizzati di gestione della contabilità l'input dei dati viene equiparato alla registrazione degli stessi nei modi tradizionali); sia la nota del Ministero delle finanze, direzione generale tasse, con la quale espressamente si afferma che l'organo accertatore — sempre nel caso che sussistano requisiti per usufruire delle disposizioni legislative per le registrazioni con macchine elettrocontabili — nelle verifiche con accesso, potrà richiedere la stampa immediata sui tabulati di quei soli dati per i quali siano già scaduti i termini di sessanta giorni per l'effettuazione delle liquidazioni e registrazioni ».

1.4. *Documento elettronico e falsità in atto pubblico.*

Atto pubblico è un termine che può essere usato in senso ristretto ovvero in senso ampio.

L'atto pubblico in senso stretto è definito dall'art. 2699 cod. civ. come il documento redatto con le richieste formalità da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato[37].

In senso ampio, invece, l'atto pubblico comprende tutti gli atti emessi dai pubblici uffici e quindi non soltanto gli atti emessi dalla pubblica amministrazione, ma anche quelli emessi dagli altri organi costituzionali e dagli organi giudiziari[38].

Fino all'entrata in vigore della legge 4 gennaio 1968 n. 15 mancava una disciplina generale della forma degli atti pubblici in senso ampio. Era tuttavia principio tradizionale che tutti gli atti pubblici dovessero essere redatti in forma scritta, dovessero indicare l'ufficio e il soggetto che li avevano emanati e dovessero contenere la data e la sottoscrizione.

La ragione di tale principio tradizionale deriva dalla funzione, principale o collaterale, di costituzione di pubbliche certezze svolta dagli atti pubblici. Gli atti e i provvedimenti amministrativi e più in genere pubblici, infatti, oltre a svolgere, secondo la loro natura, funzione di amministrazione attiva, consultiva o di controllo, hanno anche, nella gran parte, una funzione costitutiva di certezze pubbliche; la funzione cioè di rappresentare un determinato fatto o una determinata situazione giuridica e di attribuire al fatto o al rapporto così rappresentato un valore più o meno ampio di incontestabilità. Tale valore non rileva soltanto nel processo, come molto spesso si ritiene, non si identifica cioè con la probatorietà, ma ha anche un suo rilievo extra processuale e sostanzia nell'obbligo di conoscenza e di uso esclusivo ovvero impeditivo o preclusivo dell'uso di altre certezze.

La funzione di costituzione di pubbliche certezze richiede necessariamente una attività materiale di documentazione idonea a permet-

[37] Sull'atto pubblico v. CRISCI, *Atto pubblico (diritto civile)*, in *Enc. dir.*, vol. IV, p. 265; BRUGI - DOSSETTO, *Atti pubblici*, in *Noviss. Dig. it.*, vol. I, p. 1521.

[38] Sull'atto pubblico in senso ampio o documento pubblico vedi SANDULLI A., *Documento (diritto amministrativo)*, in *Enc. dir.*, vol. XIII, p. 607; sulla documentazione costituzionale vedi AMATO G., *Documentazione costituzionale*, in *Enc. dir.*, vol. XIII, p. 599; sulla documentazione amministrativa vedi GIANNINI M.S., *Diritto amministrativo*, Giuffrè, Milano, 1970 e in particolare il capo V del volume II, *I procedimenti dichiarativi*, p. 951 ss. nonché la voce *Documentazione amministrativa*, in *Enc. dir.*, vol. XIII, p. 596.

tere la conservazione dell'atto e la sua accessibilità da parte di chi vi abbia interesse. In altri termini, come si esprime la dottrina amministrativa, gli atti di certezza sono tutti ad esternazione documentale o materiale come la punzonatura, la bollatura, la sigillazione, la registrazione e, soprattutto, la redazione dell'atto in forma scritta.

Il legislatore ha sancito espressamente il principio tradizionale della necessità della forma scritta degli atti pubblici negli artt. 12 (redazione degli atti pubblici) e 13 (stesura degli atti pubblici) della legge n. 15 del 4 gennaio 1968 e ha stabilito espressamente che tutti gli atti pubblici devono essere redatti a stampa o a macchina o con scrittura a mano[39].

La funzione di costituzione di pubbliche certezze comporta non soltanto la necessità di una esternazione scritta dell'atto, ma anche la redazione di esso in più esemplari dei quali uno, o più di uno, costituiscono gli originali e gli altri le copie[40].

La redazione dell'atto amministrativo in più esemplari rende possibile la circolazione del documento. L'autorità, infatti, può rilasciare alle persone interessate gli atti che costituiscono la riproduzione integrale (copie) o parziale (estratti) del documento originale.

È necessario, tuttavia, perché la copia o l'estratto abbiano piena efficacia legale, che essi siano dichiarati autentici o conformi all'originale mediante il procedimento di certificazione. Si tratta di un procedimento amministrativo diretto alla produzione di una certezza pubblica, in cui, cioè, l'effetto di costituire una pubblica certezza non è collaterale, ma è principale e diretto e che culmina nell'emissione di un atto amministrativo detto certificato[41].

[39] Va osservato che il legislatore è forse andato oltre il segno affermando che tutti gli atti pubblici sono redatti a stampa o con scrittura a macchina e che l'articolo deve essere inteso nel senso che la redazione scritta è la formalità minima necessaria per ogni atto pubblico, salvo che la legge espressamente preveda una ulteriore o diversa forma per un atto particolare.

[40] Nel nostro ordinamento manca, ad eccezione delle norme contenute nell'art. 7 e nell'art. 14 della legge n. 15 del 1968, una disciplina generale delle copie dei documenti amministrativi e, come è stato osservato, non si sono neppure consolidate consuetudini in materia, ma piuttosto si seguono delle prassi che variano a seconda delle amministrazioni.

In genere le amministrazioni statali, ad esempio quella degli Interni e quella del Tesoro, conservano negli archivi gli originali dei provvedimenti delle autorità centrali e mettono in circolazione le copie munite di certificazione di conformità; altre amministrazioni centrali usano, invece, la pratica del doppio originale, uno per la parte e l'altro per l'archivio ministeriale; altre amministrazioni ancora conservano nell'archivio la copia conforme e fanno circolare l'originale sottoscritto dal titolare dell'ufficio che ha emesso il provvedimento.

[41] Sulla certificazione vedi STOPPANI A. *Certificazione*, in *Enc. dir.*, vol. VI, p. 769; TENTOLINI O., *Certificati e attestati*, in *Noviss. Dig. it.*, vol. III, p. 129.

In sostanza l'atto pubblico, sia esso l'atto pubblico originale, sia esso un pubblico certificato, per il nostro ordinamento giuridico deve essere sempre esternato in una forma scritta e deve normalmente essere sottoscritto dal soggetto che li ha rilasciati.

Ne consegue che un documento elettronico in senso ampio, come, ad esempio, un tabulato, può avere la particolare efficacia probatoria dell'atto pubblico o del pubblico certificato qualora sia sottoscritto dal soggetto che lo ha emesso e siano state osservate le formalità generali descritte dagli artt. 12 e 13 della legge n. 15 del 4 gennaio 1968 nonché quelle speciali previste per ciascun tipo di atto.

Un documento elettronico in senso stretto, invece, non può avere il valore di atto pubblico o di pubblico certificato: e ciò non perché non possa essere considerato anch'esso come un vero e proprio documento scritto, ma per l'impossibilità della sottoscrizione da parte del pubblico ufficiale che lo ha formato.

Attualmente, pertanto, in mancanza di una espressa norma in materia, la configurabilità dei reati di falso in atto pubblico deve essere limitata, ricorrendone gli estremi, ai documenti elettronici in senso ampio, come i tabulati sottoscritti dal pubblico ufficiale che li ha formati.

In alcuni casi, peraltro, la giurisprudenza ha ritenuto che la sottoscrizione non sia condizione dell'esistenza di un atto pubblico (Cass. 8 ottobre 1969, n. 1753; Cass. 8 febbraio 1979, n. 1049; Cass. 9 ottobre 1981, n. 701); che ci siano dei documenti in cui è possibile riconoscere con esattezza la persona o l'ente da cui lo scritto proviene (Cass. 11 febbraio 1983, n. 3310; Cass. 9 febbraio 1984, n. 8216; Cass. 10 marzo 1985, n. 5247); e che in tali casi sia da attribuire valore di pubblico documento anche all'atto non sottoscritto quando sia identificabile l'ente pubblico o il pubblico ufficiale che l'ha formato come nel caso di un orologio di un ente pubblico per la marcatura dei cartellini orario dei dipendenti (Cass. 18 ottobre 1982, n. 840) o della matrice di un biglietto ferroviario (Cass. 7 giugno 1984, n. 7722).

Inoltre è stato ritenuto che integra il reato di falso in atto pubblico il fatto di chi alteri la ricevuta di conto corrente postale attestante il pagamento della tassa di circolazione e che irrilevante è la circostanza che il documento in questione sia formato con un mezzo meccanico e sia privo di sottoscrizione. Infatti la procedura automatizzata è prevista e regolata dalla legge ed è sempre identificabile con certezza il pubblico ufficiale che ha formato l'atto[42].

[42] Nella fattispecie l'imputato aveva alterato la ricevuta di un versamento postale in conto corrente della tassa di circolazione modificandone l'importo. Circa la natura di atto pubblico e non di attestato o di certificato amministrativo trattandosi di un documento rilasciato dall'ufficiale delle poste e attestante una attività da lui svolta personalmente nell'esercizio delle sue funzioni vedi Cass. 11 dicembre 1981, n. 49, 2520; Cass. 7 luglio 1984, n. 8435; Cass. 29 gennaio 1985, n. 4412.

1.5. *Legislazioni straniere.*

L'analisi compiuta ha permesso di accertare la grande difficoltà, se non l'assoluta impossibilità, di applicare la maggior parte delle vigenti norme penali in materia di falso al documento elettronico.

La causa principale di tali difficoltà è costituita dal fatto che il documento elettronico in senso stretto non può essere considerato né scrittura privata né atto pubblico per la mancanza di una sottoscrizione.

Si impone pertanto la necessità di un'apposita normativa che provveda ad un adeguato riconoscimento del valore giuridico del documento elettronico in senso stretto e alla sua tutela anche penale.

La difficoltà di applicare le norme in materia di reati di falso ai falsi informatici è stata, del resto, avvertita non soltanto in Italia, ma anche negli altri paesi. Ad esempio in Germania la Commissione degli esperti per la lotta contro la criminalità economica ha affermato che « i dati memorizzati in un sistema elettronico non possono essere oggetto di tutela penale riconducibile allla falsificazione di atti e di certificati, in quanto non sono visivamente riconoscibili e non possono pertanto essere compresi nel concetto di atto e di certificato... ».

La stessa Commissione ha anche affermato che « per tale motivo un'alterazione dei dati memorizzati in forma elettronica non può essere perseguita penalmente sulla base della norma sancita in materia di falsificazione di atti o di certificati, nonostante il fatto che gran parte di tali dati possieda senza ombra di dubbio il carattere dell'atto o del certificato con esclusione però del requisito della riconoscibilità visiva ».

Le difficoltà di applicare ai falsi informatici le norme comuni in tema di reati di falso ha indotto quindi alcuni Paesi ad emanare apposite norme incriminatrici.

Nel Regno Unito l'art. 8 del « Counterfeiting and Forgery Act » emesso il 21 ottobre 1981 prevede che possano costituire oggetto di falsificazione anche i dati elettronici[43].

In Germania è stata invece introdotta la nuova fattispecie del reato di falso in dati rilevanti a scopi probatori consistente nella condotta di chi « al fine di inganno nei rapporti giuridici memorizza o modifica dati rilevanti a fini probatori, in modo tale che in caso di loro lettura equivarrebbero a un documento autentico ovvero falsificato » (§ 267 StGB).

[43] La norma prevede espressamente « any disc, tape, sound, track or other device on or in which information is recordered or stored by mechanical, electronic or other means ».

Negli Stati Uniti alcuni Stati prevedono due distinte fattispecie di reato: la prima consiste nel mero fatto di alterare i dati e l'altra nell'alterazione dei dati con l'intento di commettere un ulteriore reato.

Nel sistema federale, invece, sono previste come reati le alterazioni di alcune particolari specie di dati. È inoltre da ricordare la sentenza U.S. v. Jones 414, F. Supp. 964 (D.MD 1979) in cui è stato ritenuto punibile il fatto di chi sia riuscito ad ottenere, mediante l'immissione di dati falsi, l'emissione di assegni da parte dell'elaboratore.

2. Il furto informatico.

2.1. *Il furto di dati o di programmi come furto di documenti.*

Il furto di dati o di programmi può svolgersi in modi diversi che occorre tenere distinti[44].

Può verificarsi, infatti, che un soggetto si impossessi dei dati o dei programmi altrui: *a*) sottraendo il supporto cartaceo su cui sono scritti in forma tradizionale come, ad esempio, un tabulato o il listato di un programma; *b*) sottraendo il supporto informatico su cui sono memorizzati in forma di *bit* come, ad esempio, un disco magnetico o un disco ottico o anche una memoria circuitale; *c*) trasferendo abusivamente i dati dalle memorie di un sistema elettronico; *d*) accedendo abusivamente ad un sistema elettronico e prendendo così notizia dei dati e dei programmi, ma senza asportarli dal sistema stesso.

Ora non mi sembra dubbio che nella prima ipotesi possa ricorrere, sussistendo tutti gli altri estremi oggettivi e soggettivi, la tipica figura del furto di documenti.

Come è noto, infatti, « tutti i documenti... sono suscettivi di furto purché nel fatto concorrano tutti i requisiti materiali e psichici di questo reato, e specialmente quello di trarre profitto mediante l'impossessamento del documento »[45].

Più controversa è, invece, la configurabilità del reato di furto nel secondo e nel terzo caso. Potrebbe infatti obiettarsi che il documento elettronico in senso stretto non è un documento giuridico perché non è un documento scritto e che pertanto sarebbe configurabile non un un furto di documenti[46], ma eventualmente del solo supporto mate-

[44] I furti di dati o di programmi potrebbero essere forse indicati con il termine di furto informatico.

[45] Così Manzini, *Trattato di diritto penale*, Vol. IX, parte I, Utet, Torino, 1938, p. 21.

[46] Difatti, come osserva il Manzini, « Se ad una cosa manca il carattere di documento, per incompletezza, per cessazione della sua rilevanza documentale o per altro motivo, il furto in relazione ad essa rimane possibile sempre quando questa abbia un qualsiasi valore patrimoniale per se medesima (es.: carta da macero) e l'agente se ne impossessi per trarne profitto » (Manzini, *op. cit.*, p. 22).

riale su cui il documento è stato memorizzato[47]. Peraltro che anche il documento elettronico in senso stretto sia un documento giuridico è già stato affermato in materia di falso informatico e vanno quindi richiamate le osservazioni già fatte (vedi § 1, §§ 2).

Un'altra obiezione, tuttavia, è stata sollevata sopratutto in relazione ai reati di furto e di danneggiamento e va qui esaminata: e cioè che la scrittura elettronica, anche se può essere considerata una scrittura dal punto di vista funzionale, non lo è dal punto di vista materiale in quanto è composta da entità immateriali, i *bit*, non percepibili con i sensi umani. Essa, poiché immateriale, non può essere né sottratta, né danneggiata e pertanto non può essere oggetto ne del reato di danneggiamento, ne del reato di furto.

Al riguardo è stato già osservato che i *bit* che costituiscono un documento elettronico sono entità fisiche e quindi materiali pure se di natura diversa, magnetica, ottica o circuitale e anche se non percepibili con i sensi umani (cfr. § 1, §§ 2).

Questa affermazione non è in contrasto con la nozione di cosa materiale così come si è venuta a configurare nel campo del diritto penale a seguito di una evoluzione millenaria in relazione sopratutto ai requisiti della cosa oggetto di furto o di danneggiamento.

La definizione delle cose materiali e la distinzione dalle cose immateriali deriva, infatti, dalle fonti del diritto romano e precisamente da un brano delle Istituzioni di Gaio, ripreso integralmente nelle Istituzioni di Giustiniano, dove le cose materiali sono definite come le *res quae tangi possunt*[48].

[47] La distinzione è ben rilevante in quanto il supporto potrebbe essere di valore economico modesto e il documento memorizzato, invece, di grande importanza anche economica. Inoltre la distinzione è importante ai fini della configurabilità del reato di furto nei casi previsti dalla lettera *c*) in cui non si verifica l'asportazione materiale del supporto elettronico.

[48] Il titolo II del libro II delle Istituzioni di Giustiniano, intitolato *de rebus incorporalibus*, recita:

« Quaedam praeterea res corporales sunt, quaedam incorporales. 1. Corporales eae sunt, quae sua natura tangi possunt: veluti fundus, homo, vestis, aurum, argentum et denique aliae res innumerabiles. 2. Incorporales autem sunt, quae tangi non possunt, qualia sunt ea, quae in iure consistunt: sicut hereditas, ususfructus, obligationes quoquo modo contractae. Nec ad rem pertinet, quod in hereditate res corporales continentur: nam et fructus, qui ex fundo percipiuntur, corporales sunt et id, quod ex aliqua obligatione nobis debetur, plerumque corporale est, veluti fundus, homo, pecunia: nam ipsum jus hereditatis et ipsum jus utendi fruendi et ipsum jus obligationis incorporale est. 3. Eodem numero sunt jura praediorum urbanorum et rusticorum, quae et servitutes vocantur ».

« Inoltre talune cose sono incorporali, altre corporali. 1. Le corporali sono quelle che per loro natura si possono toccare, come un fondo, un uomo, una veste, l'oro, l'argento e innumerevoli altre cose. 2. Incorporali sono invece quelle che non possono toccarsi come il diritto di eredità, di usufrutto e le obbligazioni in qualunque modo contratte. E non importa che l'eredità comprenda cose corporali o che i frutti del fondo siano cose corporali o che ciò che si deve in forza di qualche obbligazione sia per lo più corporale come un uomo, un fondo o il danaro: ciò che infatti è incorporale è il diritto stesso di eredità, di usufrutto o di obbligazione. 3. Dello stesso genere sono i diritti sui fondi urbani o rustici detti anche servitù ».

La distinzione tra cose corporali o materiali che si possono toccare e le cose incorporali o immateriali che non si possono toccare è divenuta, quindi, una distinzione tradizionale e fondamentale utilizzata in ogni campo del diritto sotto vari aspetti. In particolare nel campo del diritto civile costituisce il criterio distintivo tra i beni materiali, oggetto del diritto di proprietà e degli altri diritti reali, da una parte e i beni immateriali, oggetto di diritti di esclusiva diversi come il diritto di autore o il diritto di brevetto, dall'altra; nel campo del diritto penale costituisce, invece, il criterio di delimitazione di alcuni reati che possono avere per oggetto solo beni materiali come, ad esempio, il reato di furto o di danneggiamento.

La distinzione è stata, peraltro, criticata da parte dei romanisti come una categoria ibrida in cui si confondono cose e diritti e in cui la definizione di cose corporali starebbe ad indicare piuttosto il diritto di proprietà in contrapposizione agli altri diritti di carattere patrimoniale che hanno per oggetto le cose[49]. Le *res quae tangi possunt* comprenderebbero, pertanto, tutte le cose suscettibili di impossessamento esclusivo sulle quali il soggetto può esercitare il diritto di proprietà[50].

Inoltre, mentre non vi è dubbio che all'epoca dei Romani le cose appropriabili coincidessero con le cose che potevano essere toccate, è anche vero che il progresso tecnico ha reso possibile lo sfruttamento di realtà fisiche non tangibili come i gas e le energie.

In particolare nel campo del diritto penale nel secolo scorso si è posto il problema se il gas illuminante potesse essere oggetto di furto[51]. Ed è stato affermato che esso, anche se non può essere toccato materialmente, deve tuttavia considerarsi cosa materiale e quindi suscettibile di furto in quanto comunque percepibile coi sensi. Le *res corporales* sarebbero, dunque, non soltanto le cose tangibili, ma tutte le cose comunque percepibili.

[49] Osserva al riguardo il BONFANTE; « Quanto alla distinzione romana delle *res corporales e incorporales* (Gai II, 1, 12-14; I. II, 2) essa è una categoria ibrida in cui si confondono cose e diritti. L'uso di nominare la cosa invece del diritto di proprietà, che la investe tutta, di affermare che un patrimonio abbraccia cose e diritti, si giustifica; ma la cosa non indica allora se non precisamente il diritto di proprietà, vale a dire sempre una *res incorporalis* (PIETRO BONFANTE, *Istituzioni di diritto romano*, V ed. p. 221, Vallardi, Milano).

[50] D'altra parte il verbo latino *tangere*, oltre al significato di toccare in senso materiale, può anche significare toccare in senso traslato, ossia mettere le mani sopra, appropriarsi, prendere. In tal senso Cicerone parla di *teruncium de praeda tangere* e di *nullum agrum ab invito tangere*.

[51] Le prime decisioni in tema di furto di gas sembra siano state quella di un tribunale olandese in data 3 ottobre 1850 e quella della Court of appeal inglese in data 4 giugno 1853. La questione è riferita dagli autori del tempo come *an is qui gaz dolo malo contrectat furtum faciat*.

In Italia il Carrara ricorda la decisione del Tribunale di prima istanza di Firenze in causa Ciullini e il decreto della Cassazione di Palermo in data 1 settembre 1874 contro Randazzo e Avidon (F. CARRARA, *Programma del corso di diritto criminale*, vol. IV, Firenze 1904, 7ª ed.).

Afferma al riguardo il Manzini: « Il progresso scientifico o industriale ha esteso la nozione romana delle cose corporee (*quae tangi possunt*: solidi o liquidi) anche a cose *quae tangi non possunt*, purché siano suscettive di detenzione e di impossessamento nel senso sopra precisato. Vi sono cose le quali, ancorché non abbiano forma fissa e neppure siano percepibili col tatto, si possono tuttavia detenere, e se ne può avvertire l'essenza e la presenza con un senso diverso dal tatto (materie gasose). Noi sentiamo effettivamente la loro essenza e presenza e non soltanto l'intuiamo inducendola da manifestazione mediate »[52].

Anche la nozione di res corporales come cose comunque percepibili dai sensi umani risulta, peraltro, eccessivamente restrittiva e non idonea a comprendere le energie come ad esempio l'energia elettrica ovvero i gas inodori, incolori e insapori.

La questione se le energie debbano essere considerate cose è stata risolta dal legislatore che con l'art. 624 cod. pen. ha considerato cose mobili l'energia elettrica e ogni altra energia avente un valore economico e con l'art. 814 cod. civ. ha esteso il principio a tutto il campo del diritto[53].

La configurabilità del furto di gas non percepibili con i sensi umani ha determinato un ulteriore ampliamento della nozione di res corporales. Queste vengono così a comprendere tutte le realtà materiali, solide, liquide, gassose, che siano, percepibili o anche non percepibili con i sensi umani purché sia possibile delimitarle separandole in modo assoluto e esclusivo dal mondo esterno e purché, così delimitate, siano possibile oggetto di detenzione o di possesso. Di conseguenza anche i dati contenuti in un sistema elettronico sotto forma di bit possono essere considerati cose corporali.

Può quindi ipotizzarsi un furto di documenti elettronici quando un soggetto si impadronisca dei dati e dei programmi materializzati sotto forma di bit e li sottragga a colui che li deteneva (caso di cui alla lett. *b*); e così anche nel caso di cui alla lett. *c*) nonostante che in quest'ultimo non vi sia un'apprensione materiale dell'oggetto del furto.

[52] MANZINI, *op. cit.*, p. 12.

[53] F. MANTOVANI, voce *Danneggiamento*, in *Noviss. Dig. it.*, vol. V, p. 112, Utet, Torino, 1968.

Come è noto, infatti, l'art. 624 cod. pen. non indica affatto il modo e i mezzi con cui può sottrarsi la cosa altrui. Di conseguenza la sottrazione può commettersi senza un'azione immediata dell'agente sulla cosa, ma servendosi di mezzi meccanici, chimici o fisici[54].

Il principio è magistralmente illustrato in una pagina del Carrara:

« Deve inoltre avvertirsi in ordine al soggetto passivo del furto non essere neppure necessaria la sua tangibilità. Già per principio generale sappiamo che l'uso di mezzi indiretti piuttosto che di diretti non altera l'essenzialità dei malefizi. In specie questa regola si applica al furto quando avvenga che la cosa non sia tolta al possesso altrui mercé un'azione della mano del colpevole sopra la cosa stessa, ma per virtù di un artifizio qualunque che la conduca dal possesso dell'uno nel possesso dell'altro; come si esemplifica nell'animale che adescato dal ladro passi da luogo a luogo. Per conseguenza di tali principi viene a trovarsi che la tangibilità della cosa non è requisito necessario del soggetto passivo del furto: e alla più notevole applicazione di questo vero aperse occasione nella scienza penale il progresso delle umane industrie che offrì alla città nuovi elementi di luce. Mediante clandestine introduzioni di tubi nei conduttori del gaz si operò la deviazione di quel fluido a servizio di particolari che volevano risparmiare la tassa. Fu deciso dai tribunali italiani e stranieri esaurirsi in simili fatti tutte le condizioni del furto, e fu deciso benissimo; perché sebbene la definizione contemplando i modi ordinari descriva nella *contrectatio* una operazione piuttosto soggettiva che oggettiva, nel suo spirito però non guarda all'azione diretta della mano sopra la cosa che si vuole rubare, purché si usi tal mezzo per cui la cosa medesima passi indebitamente dal possesso legittimo nello illegittimo »[55].

In sostanza, quindi, è configurabile il reato di furto e più precisamente di furto di documenti nei casi di cui alle lett. *a*), *b*) e *c*). Diverse conclusioni devono invece trarsi per il caso di cui alla lettera d) per il quale è stata talvolta usata l'espressione di furto di informazioni.

[54] V. MANZINI, *op. cit.*, p. 137. Lo stesso Autore applica i suddetti principi ai distributori automatici di cose e afferma: « Ora, chi, con qualsiasi mezzo illegittimo provoca l'azione meccanica di siffatti distributori, e in tal modo viene in possesso di cose in essi contenute, compie evidentemente una sottrazione con mezzi mediati meccanici, determinando col suo fatto l'uscita della cosa altrui dal luogo di custodia in cui si trovava rinchiusa ».

L'Autore ricorda, inoltre, « la sottrazione meccanica automatica di gas, di acqua condotta e di energia elettrica, mediante tubi o fili applicati alla conduttura in un punto anteriore a quello in cui essa entra nel contatore ».

[55] FRANCESCO CARRARA, *Programma del corso di diritto criminale*, vol. IV, p. 36, Firenze, 1904, 7ª ed.

2.2. *Il furto di dati o di programmi come furto di informazioni.*

Il furto di documenti elettronici non va confuso con il furto di informazioni ipotizzato da una parte della dottrina francese.

Difatti il furto di documenti elettronici presuppone pur sempre l'impossessamento di un oggetto materiale, e cioè del documento, anche se sotto forma di bit, e la sottrazione a colui che lo deteneva. Non è, invece, configurabile il reato di furto nell'ipotesi, frequente nella pratica, in cui un soggetto non sottragga, direttamente o indirettamente, il documento elettronico a chi lo deteneva, ma si appropri dell'informazione in esso contenuta accedendo abusivamente a un sistema elettronico.

L'informazione, infatti, è, come le idee o i diritti, una cosa immateriale e, quindi, non suscettibile di furto se priva del suo supporto materiale.

Recentemente, peraltro, è stato sostenuto nella dottrina francese che la natura immateriale dell'informazione non impedisce a priori che essa possa essere oggetto delle condotte costitutive dei delitti contro la proprietà; che non sussiste incompatibilità strutturale o di principio tra la natura dell'informazione e le fattispecie tipiche dei delitti contro la proprietà; che, quindi, è configurabile anche il furto di una informazione del tutto staccata dal suo supporto materiale[56].

In particolare questa dottrina si collega « ad una tendenza... che si manifesta in tutte le branche del diritto e che trova origine nella dematerializzazione del contenuto stesso del'attività umana...[57]; ed è sembrato che la giurisprudenza francese accogliesse questa concezione con la decisione Logabax che ha ritenuto configurabile il delitto di furto nel caso di un dipendente che aveva fotocopiato un documento confidenziale riguardante il proprio rapporto di lavoro e successivamente aveva prodotto la fotocopia così ottenuta nel corso della causa per licenziamento[58].

[56] V. l'articolo di MARIE PAULE LUCAS DE LEYSSAC, *Une Information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens?*, in *Recueil Dalloz Sirey* (1985, VIII cahier Chron. p. 43; IX cahier p. 49). Una traduzione a cura di GIOVANNA CORRIAS LUCENTE è stata pubblicata in questa *Rivista*, 1985, p. 625.

[57] M.P. LUCAS DE LEYSSAC, *op. cit.* Cfr. inoltre P. CATALA, *Les transformations du droit pénal par l'informatique*, in *Emergences du droit de l'informatique*, ed. des Parques, 1983, p. 264; *Ebauche d'une théorie juridique de l'information*, D 1984, chron p. 97, n. 5; in *Informatica e diritto*, Le Monnier, 1983, I, 15; VIVANT, *A propos des biens informationnels*, J.C.P. 1984, I, 3132.

[58] Sent. Ch. Crim. 8 gennaio 1979, D. 1979, 509 con nota di P. CORLAY; D. 1979, I.R. 182 con osservazioni di G. ROUJOU DE BOUBÉE; Gaz. Pal. 1979, 2, 501. È opportuno tuttavia tenere presente che la decisione configura il furto nella rimozione del documento originale per effettuarne la copia e non già nel solo fatto di fotocopiarlo.

Si tratta, indubbiamente di un coraggioso tentativo di ridurre « il divario manifestatosi tra ordinamento e reazione sociale conseguente all'apprensione fraudolenta dell'informazione », ma non sembra che esso possa essere accolto in base alla legislazione vigente.

Esso infatti non tiene conto del fatto che nel furto di informazione così configurato non si verifica alcuna sottrazione del bene a chi lo detiene; e che la sanzione penale finirebbe col punire la mera attività di apprensione intellettuale, indipendentemente dalla illiceità dei mezzi usati.

È pur vero che gli autori hanno tentato di limitare i confini del reato affermando che esso sussisterebbe solo nel caso di captazione fraudolenta dell'altrui informazione; e che tale captazione dovrebbe essere accompagnata o seguita da un'attività materiale che opera il trasferimento dell'informazione dal patrimonio del ladro ad un altro soggetto[59]. Senonché, in tale modo configurato, il reato appare talmente diverso dalla figura tradizionale del furto che sembra ben difficile, in mancanza di una norma espressa, poterlo considerare soggetto alle stesse norme.

La dottrina francese in tema di furto dell'informazione appare quindi più una interessante proposta per la legislazione futura che una corretta interpretazione della legislazione attuale; e allo stato deve ritenersi che sia in Francia, sia in Italia non sia configurabile un furto dell'informazione separata dalla sua materializzazione in un documento scritto, cartaceo o elettronico.

3. Il danneggiamento informatico.

3.1. *Il danneggiamento degli impianti di elaborazione dei dati.*

Il danneggiamento degli impianti informatici è stato negli anni settanta uno degli obiettivi del terrorismo che vedeva nelle nuove tecnologie un ostacolo per il suo disegno eversivo.

I numerosi casi di danneggiamento di sistemi informatici avvenuti, anche in Italia, hanno indotto il legislatore a emanare quella che forse è stata la prima norma penale in tema di informatica, la legge 18 maggio 1978, n. 191 che ha nuovamente introdotto nel codice penale il già abrogato art. 420.

Questo, nel suo testo originario disponeva: « Chiunque, al solo fine di incutere pubblico timore o di suscitare tumulto o pubblico disordine, fa scoppiare bombe, mortaretti o altre macchine o materie esplodenti, è punito, se il fatto non costituisce più grave reato, con la reclusione da sei mesi a tre anni ».

[59] M.P. Lucas de Leyssac, *op. cit.*, p. 641.

La norma, abrogata dall'art. 6, comma 2, legge 2 ottobre 1967, n. 895, è stata sostituita dall'art. 1 d.l. 21 marzo 1978, n. 59, convertito nella legge 18 maggio 1978, n. 191, con la seguente disposizione: « Chiunque commetta un fatto diretto a danneggiare o distruggere impianti di pubblica utilità o di ricerca o di elaborazione di dati, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o l'interruzione del suo funzionamento, la pena è della reclusione da tre a otto anni ».

La norma è dettata per la protezione della funzionalità degli impianti di elaborazione dei dati e quindi punisce non solo il danneggiamento dell'unità centrale, ma anche delle memorie di massa, degli organi di entrata e di uscita, dei locali e delle apparecchiature ausiliari (come ad esempio l'impianto di climatizzazione) quando il danneggiamento di questi influisca sulla funzionalità del sistema di elaborazione nel suo complesso.

Parimenti alcune decisioni giurisprudenziali hanno ritenuto applicabile la norma anche nel caso in cui il danneggiamento, pur avendo come oggetto i dati o i programmi, è, tuttavia, di tale gravità da incidere sulla funzionalità dell'intero sistema di elaborazione: così, ad esempio,nel caso che il danneggiamento riguardi il sistema operativo ovvero la totalità o una gran parte dei programmi applicativi.

Tra le prime decisioni in materia vanno ricordate la sentenza dell'Ufficio Istruzione di Torino 12 dicembre 1983[60] e la sentenza dell'Ufficio Istruzione di Firenze 27 gennaio 1986[61].

In particolare quest'ultima, in un caso in cui mediante l'uso di magneti erano state causate numerose alterazioni e menomazioni di dischi in uso presso l'elaboratore dati del centro di calcolo di una Università, ha affermato che « costituiscono atti genericamente qualificabili di sabotaggio di un impianto di elaborazione dati quelle alterazioni magnetiche che rendono impossibile l'accesso e l'utilizzo delle informazioni memorizzate in dischi così da risultare in pratica distrutte, anche se il danno arrecato ai supporti possa considerarsi riparabile ».

La decisione è stata criticata da un autore, il Picotti per il quale in nessun caso il danneggiamento dei dati o dei programmi può ricadere nella previsione di cui all'art. 420 cod. pen.: e ciò anche nel caso di fatti che incidano sulla funzionalità stessa del sistema elettronico.

[60] In *Giur. it.*, 1984, II, p. 351 con nota di A. FIGONE, *Sulla tutela penale del* software.

[61] In questa *Rivista*, 1986, p. 962 con nota di L. PICOTTI, *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dei dati*; in *F.I.* 1986, II, p. 359 con nota di C. RAPISARDA.

Osserva al riguardo l'Autore che l'oggetto materiale del reato di cui all'art. 420 cod. pen. è « ... espressamente circoscritto ai soli impianti ...; e che « ... il restringimento della onnicomprensiva nozione di cosa ai soli impianti e l'espunzione dalla previsione penale precisamente di quelle forme di condotta che più direttamente tutelano l'integrità della cosa di fronte a fatti che non ne pregiudicano tanto la sostanza materiale quanto la mera utilizzabilità funzionale (vale a dire la dispersione o la inservibilità totale o parziale, affiancate alla distruzione e al danneggiamento oltreché allo stesso deterioramento nell'art. 635 cod. pen.) rendono ancora più discutibile l'applicazione, a fatti aggressivi del solo *software*, della nuova fattispecie di attentato rispetto a quella comune di danneggiamento »[62].

Lo stesso Autore osserva che « a prescindere dal riconoscimento che un'alterazione magnetica difficilmente integra di per sé un danneggiamento o una manomissione del supporto materiale (disco o altro) e tantomeno dell'impianto in cui avviene, si pone quindi comunque il problema di garantire la tutela dei dati o dei programmi in quanto tali... indipendentemente dalla perdurante integrità ed idoneità funzionale dell'*hardware* e non solo quando sono memorizzati sui supporti (magnetici o di altro genere), ma anche durante tutte le fasi di elaborazione, riproduzione e sopratutto trasmissione a distanza »[63].

Non sembra, tuttavia, che la tesi dell'autore possa essere del tutto condivisa. Difatti il termine impianti è un termine molto generale che indica « l'insieme di apparecchi, attrezzature, congegni ecc. concorrenti a uno stesso scopo o indispensabili per un determinato fine »[64]; un impianto di elaborazione dati non può essere considerato composto dalle sole macchine, ma dall' insieme di macchine, dati e programmi; e il legislatore ha voluto tutelare la funzionalità degli impianti di elaborazione dei dati non soltanto contro gli atti di distruzione fisica, ma anche contro quegli atti più sofisticati che incidono sui dati o sui programmi.

Questa interpretazione più ampia dell'art. 420 cod. pen. è stata recentemente confermata dalla sentenza del Pretore di Torino 23 ottobre 1989[65] che ha ritenuto sussistente il reato di danneggiamento di cui all'art. 635 cod. pen. nel caso di un tecnico che, incaricato da

[62] L. PICOTTI, *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dei dati*, in questa *Rivista*, 1986, p. 969.

[63] L. PICOTTI, *ibid.*

[64] *Dizionario enciclopedico italiano*, vol. VI, p. 80, Istituto della Enciclopedia italiana, Roma, 1957.

[65] In questa *Rivista*, 1990, p. 620, con nota di richiami di dottrina e di giurisprudenza a cura di GIOVANNA CORRIAS LUCENTE.

una ditta della manutenzione del proprio sistema informativo, aveva cancellato dei nastri di *back-up* e aveva introdotto una serie di istruzioni nel programma idonee a disabilitare il sistema ad una data prestabilita; e ciò per il timore che la ditta, non contenta dell'assistenza sistematica, si potesse rivolgere ad un'altra società di assistenza.

Più precisamente il Pretore ha ritenuto che l'alterazione fisica del nastro ovvero l'introduzione di un programma *killer* per la disabilitazione delle procedure avrebbero messo la ditta committente nell'impossibilità di ripristinare le procedure di gestione e, in sostanza, di utilizzare i dati memorizzati; avrebbero, cioè, reso inservibile il bene costituito dal sistema informativo che è costituito dall'unità inscindibile della base dei dati, dei programmi e dei supporti fisici (dischi, nastri, elaboratore).

Del resto anche in alcuni ordinamenti giuridici stranieri il legislatore ha configurato una nozione di danneggiamento di impianti informatici molto ampia e comprensiva quindi non solo delle macchine nella loro materialità, ma anche dei dati e dei programmi necessari per il funzionamento del sistema. In particolare nell'ordinamento giuridico tedesco sono state introdotte due figure di danneggiamento informatico: la manomissione del dati e il vero e proprio sabotaggio informatico (§§ 303a e 303b StGB).

Il primo punisce con la detenzione fino a due anni o con una pena pecuniaria « chiunque illegittimamente cancella, sopprime, rende inutilizzabili o manomette dati ».

Il secondo, invece, punisce con la detenzione fino a cinque anni o con una pena pecuniaria « chiunque disturba un procedimento di elaborazione dati, che sia di essenziale significato per un'azienda o un'impresa altrui o per una pubblica amministrazione, mediante: 1) la commissione di un atto conforme alle previsioni di cui al § 303a comma 1; ovvero 2) la distruzione, il danneggiamento, la rimozione, la manomissione o il rendere inutilizzabile un impianto di elaborazione dati o un supporto informatico[66].

[66] Sulla legge tedesca vedi l'articolo di L. PICOTTI, *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dei dati*, in questa *Rivista*, 1986 p. 969.

3.2. *Il danneggiamento di dati e di programmi come danneggiamento di documenti.*

I casi di danneggiamento di dati o di programmi sono ancora più diffusi dei danneggiamenti che hanno per oggetto le macchine.

Le ragioni di tale fenomeno sono le più varie: il puro spirito vandalico o l'interesse commerciale come, ad esempio, nel caso dei cosiddetti « virus »; la illecita concorrenza; lo spirito di vendetta di un dipendente, più o meno giustamente licenziato; perfino l'interesse della società addetta alla manutenzione di un sistema di impedire ad altri di sostituirla in questa attività.

Come abbiamo già visto, quando il danneggiamento, pur avendo come oggetto i dati o i programmi, è, tuttavia, di tale gravità da incidere sulla funzionalità del sistema di elaborazione può ritenersi applicabile l'art. 420 cod. pen.: così, ad esempio,nel caso che il danneggiamento riguardi il sistema operativo ovvero la totalità o una gran parte dei programmi applicativi.

Quando, invece, il danneggiamento riguardi una parte limitata di dati ovvero alcuni programmi applicativi di importanza minore non è configurabile l'ipotesi di cui all'art. 420 cod.pen. e in dottrina sono state sollevate molte obiezioni circa l'applicabilità dell'art. 435 cod. pen. che punisce chi « distrugga, disperda, deteriori o renda inservibili cose mobili altrui ».

Le difficoltà di applicazione della norma derivano, al pari della questione della configurabilità del reato di furto, dalla ritenuta natura non materiale dei dati e dei programmi; pertanto le stesse osservazioni fatte in tema di furto possono qui intendersi ripetute; e deve ritenersi che, come è configurabile il furto di documenti elettronici contenenti dati o programmi anche sotto forma di bit su supporti circuitali o magnetici, così parimenti è configurabile il reato di danneggiamento di documenti elettronici[67].

Al riguardo va nuovamente ricordata la già menzionata sentenza del Pretore di Torino 23 ottobre 1989[68] che ha ritenuto sussistente il reato di danneggiamento di cui all'art. 635 cod. pen. nel caso di un tecnico che, incaricato da una ditta della manutenzione del proprio sistema informativo, aveva cancellato dei nastri di *back-up* e aveva introdotto una serie di istruzioni nel programma idonee a disabilitare il sistema ad una data prestabilita; e ciò per il timore che la ditta, non contenta dell'assistenza sistematica, si potesse rivolgere ad un'altra società di assistenza.

[67] Difatti, come osserva il MANZINI, « ...sono suscettivi di danneggiamento tutti quei documenti che possono divenire oggetto di furto... a parte i caratteri differenziali del danneggiamento dai delitti specifici di soppressione, ecc., di documenti, preveduti negli artt. 255 e 490... » (V. MANZINI, *op. cit.*, p. 435).

[68] Vedi nota 65.

In particolare il Pretore ha ritenuto che l'alterazione fisica del nastro ovvero l'introduzione di un programma *killer* per la disabilitazione delle procedure avrebbero messo la ditta committente nell'impossibilità di ripristinare le procedure di gestione e nella sostanza di utilizzare i dati memorizzati; avrebbero, cioè, reso inservibile il bene costituito dal sistema informativo che è costituito dall'unità inscindibile della base dei dati, dei programmi e dei supporti fisici (dischi, nastri, elaboratore).

La parte più importante della decisione, peraltro, è quella in cui il Pretore ha ritenuto che indipendentemente dalla sua incidenza sul sistema, « la cancellazione dei nastri può essere considerata a tutti gli effetti una alterazione fisica del supporto magnetico. Quest'ultimo, infatti, esplica la propria funzionalità sulla base dell'informazione memorizzata su di esso, informazione che è codificata in ultimo mediante una variazione sia pur microscopica delle proprietà chimico-fisiche del mezzo ».

La decisione mi sembra di grande importanza: con essa infatti non soltanto si afferma l'applicabilità dell'art. 420 cod. pen. ai casi di danneggiamento di dati e di programmi quando questo incida sulla funzionalità del sistema di elaborazione dei dati, ma si afferma per la prima volta la configurabilità del reato di danneggiamento dei dati e dei programmi anche al di fuori dell'ipotesi di cui all'art. 420 quando cioè il danneggiamento non incida sul funzionamento del sistema.

Va tuttavia osservato che sia il nastro sia il disco magnetico sono destinati per loro natura ad essere utilizzati più volte e che pertanto il danneggiamento non consiste nella modificazione fisica del nastro o del disco in quanto tale, ma nella cancellazione del documento in esso memorizzato. In definitiva anche in questa ipotesi è configurabile solo un caso di danneggiamento del documento sia pure memorizzato sotto forma digitale.

4. L'ACCESSO E L'UTILIZZAZIONE ABUSIVI DI UN ELABORATORE.

L'accesso abusivo a un elaboratore può avvenire in vari modi: mediante l'ingresso abusivo del soggetto nei locali ove è situato l'elaboratore; attraverso la falsificazione dei dispositivi di accesso al sistema come, ad esempio, l'uso non autorizzato di un codice o di una carta elettronica; attraverso l'inserimento abusivo in una rete telematica.

L'accesso abusivo può essere compiuto non solo allo scopo di impadronirsi di dati o di programmi ovvero di utilizzare le memorie o l'unità centrale dell'elaboratore, ma anche per motivi di mero gioco, come, ad esempio, nel caso dei cosiddetti *hackers* oppure allo scopo di commettere ulteriori reati.

Nel nostro ordinamento, in mancanza di una apposita norma incriminatrice, si è tentato di ricondurre le ipotesi di accesso abusivo alle figure tradizionali di reato come la violazione di domicilio previ-

sta dall'art. 614 cod. pen., i reati di falsità personale e, in particolare, la sostituzione di persona prevista dall'art. 494 cod. pen., l'intercettazione delle comunicazioni telefoniche e telegrafiche prevista dall'art. 632-*bis* cod. pen.; e si è persino parlato di peculato d'uso nel caso di uso illecito di un elaboratore della pubblica amministrazione da parte di un pubblico dipendente.

Nessuna di tali ipotesi peraltro sembra perfettamente applicabile.

Infatti l'oggetto del reato di violazione di domicilio è la tutela della pace domestica e della privata dimora. La norma è stata estesa dalla giurisprudenza agli studi professionali, alle banche e alle scuole, ma certamente non si applica agli stabilimenti industriali, alle officine, ai laboratori, agli esercizi e agli uffici pubblici; e non si applica neppure nei confronti delle persone ammesse all'interno dei locali come, ad esempio, i dipendenti quando essi ne approfittino per svolgere attività non lecita.

Il reato di sostituzione di persona, invece, richiede l'induzione in errore di una persona e non può consistere nel fornire false indicazioni ad una macchina, quand'anche questa operi di conseguenza.

I reati di intercettazione di dati di cui agli artt. 617 e seguenti del codice prevedono e puniscono le intercettazioni di comunicazioni e di conversazioni telegrafiche e telefoniche che avvengono tra due o più persone rispetto alle quali l'intercettatore è un terzo, ma non possono applicarsi nei casi di intercettazione di un messaggio tra un elaboratore ed un soggetto e, tantomeno, nei casi in cui « l'agente pone in essere, seppur arbitrariamente, una relazione di natura interattiva con l'elaboratore nel cui ambito assume la veste di mittente o di ricevente e pertanto di soggetto che, per esplicita esclusione legislativa, non è destinatario della norma incriminatrice »[69]. Infine non sembra applicabile l'ipotesi del peculato d'uso tranne, forse, nei riguardi degli elaboratori della pubblica amministrazione quando l'uso abusivo abbia comportato « un significativo impegno della memoria elaboratore tale da precluderne l'integrale disponibilità per il perseguimento della pubblica destinazione »[70].

Le difficoltà incontrate nell'applicazione delle figure tradizionali di reato hanno indotto alcuni autori a tentare più ardite costruzioni dottrinali e a ipotizzare le figure di furto o di appropriazione indebita di informazioni o di servizi informatici in contrasto con il tradizionale principio della materialità della cosa oggetto di tali reati e con conseguenze dirompenti dell'intero sistema dei reati patrimoniali; ovvero la figura del furto d'uso nel caso di abusiva utilizzazione delle memorie o del tempo macchina dell'elaboratore.

[69] G. Corrias Lucente, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in questa *Rivista*, 1987, p. 195.

[70] G. Corrias Lucente, *op. cit.*, p. 201.

Le stesse difficoltà di inquadramento delle nuove fattispecie nelle figure tradizionali di reato sono state incontrate negli altri paesi europei e negli Stati uniti d'America; infatti in quest'ultimo paese molti stati hanno emanato un'apposita normativa per la punizione del reato di accesso abusivo ovvero del furto di servizi di un elaboratore.

A livello federale, invece, il Counterfeit Access Device and Computer Fraud Act del 1984 prevede come reato tre ipotesi di accesso abusivo: l'accesso abusivo qualificato dall'intento di apprendere informazioni riservate sull'applicazione dell'energia atomica, sulla difesa o la politica estera degli Stati uniti e dall'ulteriore scopo di danneggiare gli Stati uniti o di favorire un paese straniero; l'accesso abusivo diretto ad ottenere informazioni finanziarie; l'accesso abusivo che ha comportato l'apprensione, la distruzione o la rilevazione di dati contenuti in elaboratori del Governo[71]. Al di fuori di tali specifiche ipotesi e delle altre previste dall'Electronic Fund Transfer Act e dal Credit Card Fraud Act l'uso non autorizzato degli elaboratori non costituisce reato[72].

In Italia manca qualsiasi norma in materia ad eccezione dell'art. 12 della legge n. 197/1991. Pertanto, al di fuori dell'ipotesi prevista in quest'articolo[73], non vi è alcuna tutela penale nei confronti degli accessi abusivi a un elaboratore se non nei limiti in cui siano applicabili le norme penali in tema di segreti ovvero quelle a tutela del diritto di autore, di brevetto e degli altri segni distintivi dei prodotti commerciali.

4.1. *La tutela penale del segreto.*

Il codice penale contempla in varie norme la violazione dei segreti. Tra i delitti contro la personalità dello Stato prevede e punisce la violazione dei segreti politici e militari (art. 256 ss., cod. pen.); tra i delitti dei pubblici ufficiali contro la pubblica amministrazione prevede e punisce la violazione dei segreti di ufficio (artt. 325 e 326 cod. pen.); infine, tra i delitti contro la libertà individuale prevede e puni-

[71] Il testo della legge è riportato in appendice.

[72] Sono stati tuttavia presentati al Parlamento federale alcuni progetti di legge che prevedono come reato l'accesso abusivo ad un elaboratore per ottenere servizi.

[73] Vedi § 5, §§ 2.

sce i delitti contro la inviolabilità dei segreti (artt. 616-623 cod. pen.)[74].

In materia di informatica particolare importanza presenta l'art. 621 cod. pen. che prevede e punisce la rivelazione e l'impiego del contenuto di documenti segreti. La norma, infatti, può essere applicata nei casi di rivelazione o di impiego di dati o di programmi elettronici o, più in generale, di documenti elettronici.

Occorre, tuttavia, che ricorrano tutti i presupposti oggettivi e soggettivi della norma e, innanzitutto, che si tratti di un segreto[75]; occorre, cioè, che i dati o i programmi rivelati o impiegati non siano noti e il titolare del diritto al segreto non abbia, esplicitamente o implicitamente, rinunciato al segreto stesso[76]. La norma è, dunque, applicabile nei soli casi in cui i dati o i programmi siano tenuti segreti dal titolare e un altro soggetto ne sia venuto abusivamente a cognizione; non è applicabile, invece, nel caso in cui i dati o i programmi siano destinati ad essere comunicati o diffusi o comunque commercializzati.

Un' altra forma di tutela penale dei dati o dei programmi potrebbe essere assicurata dall'art. 623 cod. pen. che prevede e punisce la rivelazione di segreti scientifici o industriali. Occorre, tuttavia, osservare che la norma parla di scoperte, invenzioni scientifiche o applicazioni industriali ossia di quei beni che possono costituire oggetto di brevetto e che la disciplina penale ha una funzione strumentale e complementare rispetto a quella del brevetto: strumentale in quanto il diritto di brevetto « presuppone il precedente segreto, dato che la divulgazione anteriore alla domanda di brevetto, facendo venire meno il requisito della novità, rende il brevetto invalido »[77]; complementare

[74] Dispone precisamente l'art. 621 cod. pen. (rivelazione del contenuto di documenti segreti): « Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela , senza giusta causa, ovvero l'impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da lire duecentomila a due milioni.

Il delitto è punibile a querela della persona offesa ».

Dispone, invece, l'art. 622 cod. pen. (rivelazione di segreto professionale): « Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione.

Il delitto è punibile a querela della persona offesa ».

Dispone, infine, l'art. 623 cod. pen. (rivelazione di segreti scientifici o industriali): « Chiunque, venuto a cognizione in ragione del suo stato o ufficio o della sua professione o arte, di notizie destinate a rimanere segrete sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto è punito con la reclusione fino a due anni.

Il delitto è punibile a querela della persona offesa ».

[75] CRESPI, *La tutela penale del segreto*, p. 7, Palermo, 1952.

[76] ANTOLISEI F., *op. cit.*, p. 164.

[77] ANTOLISEI F., *op. cit.*, p. 174. L'Autore aggiunge: « Insomma il diritto di brevetto, se deriva dalla creazione, si conserva solo mediante il segreto. Di qui la necessità che tale segreto sia protetto penalmente » (*ibid.*).

in quanto assicura la tutela dell'invenzione o della scoperta o dell'applicazione industriale nei casi in cui l'inventore preferisca conservare il segreto, anziché chiedere il brevetto. La norma presuppone dunque una scoperta, un'invenzione scientifica o un'applicazione industriale; e pertanto quando i dati o i programmi non costituiscano uno di tali beni, non potrà essere applicato l'art. 623 cod. pen., ma, semmai, il precedente art. 622 che prevede e punisce la rivelazione del segreto professionale.

La distinzione è ben rilevante. Infatti l'art. 622 subordina la punibilità del fatto al verificarsi di un nocumento e concerne solo le notizie che debbono rimanere segrete a differenza dell'art. 623 che non richiede né l'effettivo verificarsi né la semplice possibilità di verificarsi del danno.

D'altra parte sia l'art. 622 sia l'art. 623 non assicurano una tutela generale che possa essere fatta valere nei confronti di tutti, ma solo una tutela che può essere fatta valere nei confronti di determinati soggetti. Essa, infatti, è « concessa solo verso persone che siano pervenute a conoscenza delle notizie destinate a rimanere segrete a cagione della loro professione, e non anche verso i terzi i quali si siano procurati la conoscenza medesima »[78]. La tutela penale è quindi applicabile solo nell' ipotesi in cui un soggetto sia venuto a conoscenza dei dati o dei programmi per ragioni professionali, come, ad esempio, nel caso di un dipendente di una casa produttrice di programmi; al di fuori di tale ipotesi non è in grado di assicurare una tutela penale generale e efficace in tutti gli altri casi di accesso illecito o abusivo ai dati o ai programmi di un elaboratore.

Può essere interessante osservare che sotto tale aspetto la disciplina del segreto commerciale (*trade secret protection*) negli Stati Uniti d'America è analoga a quella italiana.

La tutela del segreto commerciale, infatti, risale ai precedenti di *common law* di ciascuno Stato[79] ed è subordinata alla presenza di quattro requisiti: idoneità dell'oggetto (*appropriateness of subject matter*); *b*) carattere di segretezza (*secrecy*); carattere di novità (*novelty*); *d*) rilevanza economica (*economic value*).

[78] ANTOLISEI F., *Manuale di diritto penale*, parte speciale, vol. I, 3ª ed., p. 172, Giuffrè, Milano, 1957.

[79] V., ad esempio, Dupont Power Co., v. Masland, 244, U.. 100, 102 (1917).

Negli Stati Uniti, pertanto, la tutela del segreto commerciale è stata applicata solo nei casi in cui un dipendente sia pervenuto per ragioni professionali a conoscere dati o programmi destinati a rimanere segreti.

I rapporti di lavoro, infatti, prevedono spesso clausole (*contractual agreements*) con le quali il dipendente si obbliga a non comunicare o divulgare informazioni riservate e a non svolgere, durante o dopo il rapporto, attività concorrenziali.

Le informazioni riservate riguardano, in genere, oltre alla lista dei clienti e dei fornitori, le innovazioni dei sistemi di produzione e le notizie relative ai programmi per elaboratori; e tra gli obblighi di non svolgere attività concorrenziale è spesso previsto espressamente quello di non svolgere attività di programmazione per conto proprio o di terzi.

La giurisprudenza ha precisato che queste clausole operano anche quando il dipendente non abbia sottratto programmi redatti su supporti materiali, ma si sia valso soltanto della propria memoria per scrivere programmi identici o simili[80]; esse, comunque, presuppongono un rapporto di lavoro e non operano quando questo manchi.

Quest'ultimo principio è stato chiaramente espresso nella decisione Republic Systems and Programming, Inc. v. Computer Assistance, Inc. La Republic svolgeva attività di *software house* mediante programmatori assunti non già con rapporto di lavoro subordinato (*employment contract*), ma con contratti di lavoro autonomo (*contract programming*). Uno dei suoi programmatori, Andrew Vignale, decise di formare una propria *software house*; assunse 20 dei 25 programmatori della Republic e contattò tutti i clienti di questa per offrire i servizi della nuova società. La Republic citò Vignale per violazione dell'obbligo di fedeltà (*breach of fiduciary duty*) e per appropriazione di segreti commerciali (*misappropriation of trade secrets*) e cioè delle liste dei clienti. La Corte respinse la domanda affermando che il Vignola non era un dipendente e quindi non aveva altri obblighi nei confronti della Republic oltre quello di effettuare l'opera commessagli; di conseguenza era libero di assumere gli impiegati della Republic e di contattare clienti; né tali dati potevano essere considerati segreti commerciali in quanto la lista dei clienti era pubblicata sui *depliant* della compagnia a titolo di pubblicità[81].

Il principio è stato ulteriormente precisato dalla decisione Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp. che ha affermato che non sempre un rapporto di lavoro subor-

[80] Ah Emery Co. v. Marcond Product Co., 393 U.S. 835 (1968); Sperry Rand Corp. v. Rothlien, 241, F. Supp. 549 (D Conn 1964).

[81] Republic System and Programming Inc. v. Computer Assistance, Inc., in 322 F. Supp. 619 (D Conn 1970).

dinato implica un obbligo di segreto. Infatti occorre distinguere il caso in cui la redazione del *software* rientri o sia connessa con l'attività espletata dal dipendente, dal caso in cui il programma sia creato dal dipendente nel proprio tempo libero e indipendentemente dalle conoscenze specifiche acquisite durante il lavoro; inoltre vi possono essere dei casi in cui l'obbligo di fedeltà e quindi del segreto sussiste non in forza di un rapporto di lavoro subordinato, ma « on agency principles or on specific dealing between parties in which a situation of trust arises and out of which sought-to-be protected knowledge is acquired ».

4.2. *La tutela penale del diritto d'autore.*

L'ordinamento giuridico prevede, oltre a una tutela civile, anche una tutela penale del diritto di autore mediante la previsione come reati di alcune figure tipiche di lesione di tale diritto.

In particolare l'art. 171 della legge sul diritto di autore prevede e punisce come delitti e, qualora siano commesse per colpa, come contravvenzioni, la pubblicazione o la riproduzione abusiva di un'opera altrui.

La stessa norma prevede, inoltre, un' altra serie di figure delittuose come la diffusione e la messa in vendita abusiva di un' opera altrui e l'introduzione nello Stato di esemplari prodotti all'estero contrariamente alla legge italiana (art. 171 lett. *a*); la rappresentazione abusiva di un'opera altrui adatta a pubblico spettacolo o l'esecuzione abusiva di una composizione musicale (art. 171 lett. *b*); l'elaborazione illecita (art. 171 lett. *c*), la duplicazione e lo smercio illecito di dischi e di altri apparecchi analoghi (lett. *e*), la ritrasmissione abusiva e la registrazione abusiva di emissioni radiofoniche (lett. *f*)[82],

La legge prevede poi una pena più grave, la reclusione fino a un anno (in alternativa con la multa), se i reati sono commessi sopra un'opera altrui non destinata alla pubblicità ovvero con usurpazione della paternità dell'opera ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima qualora ne risulti offesa all'onore o alla reputazione dell'autore (art. 171 u.c.)[83].

Il sistema penale di protezione del diritto di autore non è andato esente da critiche. È stato, ad esempio, osservato che l'art. 42 u.c. cod. pen. dichiara che nelle contravvenzioni ciascuno risponde della propria azione od omissione, cosciente e volontaria, sia essa dolosa o

[82] L'art. 203 dispone che, finché non saranno emanate con decreto presidenziale norme particolari per disciplinare il diritto esclusivo di televisione, esso sarà regolato dai principi generali della legge sul diritto di autore in quanto applicabili.

[83] L'art. 172 aggiunge, peraltro, che se i fatti sono commessi per colpa, la pena è dell'ammenda sino a lire ottantamila.

colposa; che i medesimi fatti non possono quindi considerarsi delitti o contravvenzioni a seconda che sussista o meno il dolo dell'agente; e che la distinzione dovrebbe essere basata, secondo la proposta di Piola Caselli, sull'esistenza o meno del fine di lucro o dell'intenzione di nuocere[84].

La normativa, peraltro, si manifesta particolarmente carente in quanto non prevede le moderne forme di illecita riproduzione delle opere di ingegno altrui come, ad esempio, le fotocopie ovvero la riproduzione di brani televisivi o musicali mediante le cosiddette « cassette » o « videocassette ».

La legge 29 luglio 1981 n. 406 ha previsto altre ipotesi delittuose consistenti nell'abusiva riproduzione a fini di lucro o messa in commercio di dischi, nastri o supporti analoghi.

Il sistema peraltro si manifesta ancora carente in particolare nel campo dell'informatica e della tutela dei dati e dei programmi. Le norme penali in tema di diritto di autore, infatti, in tanto potrebbero essere applicate in questo campo in quanto sia considerato il programma come un'opera dell'ingegno.

Senonché la natura dei programmi è, come noto, controversa in dottrina e in giurisprudenza. Difatti mentre la giurisprudenza civile ha più volte affermato la natura del programma per elaboratore come opera dell'ingegno, la giurisprudenza penale lo ha più volte negato e ha di conseguenza negato che potessero essere applicate le norme penali sul diritto di autore[85].

Tra le sentenze che hanno escluso la tutela penale dei programmi vanno ricordate quelle decisioni che hanno affermato che i videogiochi non possono inquadrarsi tra le opere dell'ingegno appartenenti all'arte cinematografica e non può pertanto apprestarsi loro la tutela penale di cui all'art. 171 legge n. 633/1941 (Pretura di Milano 1° giugno 1982, Pretura di Padova 15 dicembre 1983); che i program-

[84] E. Piola-Caselli, A. Arienzo e F. Bile, *Diritti d'autore*, voce del *Noviss. Dig. it.*, vol. V, p. 705, Utet, Torino, 1968.

[85] Un'ampia rassegna della dottrina e della giurisprudenza sulla natura giuridica dei programmi per elaboratori è contenuta nell'opera di R. Ristuccia e V. Zeno-Zencovich, *Il software nella dottrina e nella giurisprudenza*, Cedam, Padova, 1990 in cui è riportato, tra l'altro, il testo integrale delle decisioni citate nel testo.

mi per elaboratore ed in particolare i programmi residenti i quali presentano una forma vincolata dal microprocessore non costituiscono opera letteraria in quanto quest'ultima deve sempre considerarsi indirizzata all'uomo e che non costituisce reato perché non previsto dalla legge come tale il fatto di chi riproduca il programma residente di un elaboratore elettronico in quanto ad esso non è estensibile, stante il divieto dell'analogia, il disposto dell'art. 171 legge aut. (Pretura di Bologna 24 aprile 1986); che la copia pedissequa di un programma per elaboratore elettronico e, in particolare del sistema operativo di quest'ultimo, non è sanzionabile penalmente perché il fatto non è previsto dalla legge come reato in quanto mentre in materia civile è ammessa un'interpretazione analogica che permetta di considerare il *software* opera dell'ingegno anche al di fuori dell'elencazione contenuta negli artt. 1 e 2 della legge sul diritto di autore, ciò non è ammesso in sede penale; ne è accoglibile un'interpretazione estensiva di opera letteraria tale da comprendere anche i programmi per elaboratore (Pretura di Monza 26 luglio 1985)[86].

Va tuttavia tenuto presente che, anche se la grande maggioranza dei giudice di merito tende ad escludere la sussistenza del reato, una decisione della Corte di Cassazione 24 novembre 1986 ha affermato che i programmi per elaboratore sono tutelati civilmente e penalmente dalla normativa sul diritto di autore in quanto opere dell'ingegno che appartengono alle scienze e si esprimono in linguaggio tecnico-convenzionale concettualmente parificabile all'alfabeto o alle sette note[87].

[86] Pret. Monza 26 luglio 1985 (Pretore D'Aietti - Imp. Crespi).

In particolare il Pretore osserva:

« ...appare evidente che nel nostro ordinamento la norma incriminatrice penale non può estendersi ai programmi per elaboratori elettronici se non attraverso una interpretazione che faccia leva sull'analogia.

Infatti va esclusa la possibilità di configurare una semplice interpretazione estensiva; l'opera letteraria, che il diritto di autore intende tutelare, non può ricomprendere, nella sua accezione terminologica, anche un programma sorgente costituito da una serie di algoritmi matematico-formali che, in quanto strettamente funzionali alla funzione operativa che debbono svolgere, sono privi di ogni e qualsiasi contenuto letterario; opinando altrimenti potrebbe ricomprendersi nell'opera letteraria anche lo spartito musicale che è pure redatto in un linguaggio simbolico formale ma che, unanimamente, è ricompreso in una distinta categoria di opere d'ingegno.

Poiché l'interpretazione analogica in malam partem non è ammessa nel nostro sistema penale se ne trae la conseguenza che deve emettersi sentenza di non doversi procedere nei confronti dell'imputato E.C.

È evidente che un diverso discorso potrebbe essere fatto sotto il profilo strettamente civilistico ove l'interpretazione analogica è ammessa e trova un più ampio spazio applicativo. Ma trattandosi di un procedimento penale, pur riconoscendosi l'esistenza di una plateale operazione di copia di programmi, non si ritiene di poter configurare un plagio sanzionabile penalmente.

Analoga soluzione si ottiene nell'ipotesi che si propenda per l'applicabilità della fattispecie di cui all'art. 99 della legge sul diritto d'autore il quale postula la esistenza di un diritto di chiunque di utilizzare, anche senza il consenso dell'autore, il progetto tecnico di costui al fine di eseguirlo.

Tale attività di utilizzazione non è, quindi, vietata ai sensi della legge sul diritto d'autore e non può essere sanzionata in alcun modo potendosi al più da parte degli autori pretendere l'equo compenso ».

[87] Cassazione sezione terza penale (Presidente Garella - Estensore Montoro - Ricorrente SIAE).

In particolare la Corte ha affermato:

« L'analista di sistemi, che determina la metodologia necessaria per l'elaborazione delle informazioni, ed il programmatore, che scrive nel modo più opportuno le istruzioni che costituiscono il programma — specializzazioni che spesso coesistono nella stessa persona — si avvalgono entrambi di un linguaggio tecnico-convenzionale, concettualmente parificabile all'alfabeto per chi scrive o alle sette note per il musicista, etc.; ma similmente a costoro, in tanto producono un risultato creativo in quanto diano apporti nuovi nel campo informatico, esprimano soluzioni originali ai problemi di elaborazioni dei dati, programmino in modo migliore rispetto al passato determinati contenuti di idee, seppure in misura appena apprezzabile.

Il nuovo nell'espressione formale di un contenuto ideativo — allora — è il discrimine di proteggibilità anche per il *software*, sicché non sono oggetto di protezione tutte le attività preparatorie non collegate all'elaborazione della sintesi creativa e quelle esclusivamente riproduttive di elementi già noti e sfruttati, per così dire, il già visto.

In ultimo è appena il caso di dire come anche in Italia l'inquadramento del *software* nella categorie delle opere che appartengono alle scienze segue, ogni giorno di più, l'evoluzione culturale in riferimento al progresso tecnico o scientifico.

Del resto l'informatica in genere, e quella giuridica in specie, sono ormai divenute materie di insegnamento secondario e universitario; e, comunque, sarebbe al di fuori del tempo presente se opere di così sofisticato impegno culturale (in senso classico ed in quello sociologico) non potessero essere comprese nelle classificazioni — per altro — non tassative per lungimirante scelta del legislatore.

Il software è — dunque — oggetto del diritto di autore, protetto civilmente e penalmente dalle norme ricordate; ne può essere altrimenti — vale a dire tutelabile con i rimedi previsti dal codice civile in favore delle invenzioni industriali e contro l'imitazione servile dei prodotti, come è stato pure sostenuto — per esplicita esclusione legislativa, giacché il d.P.R. 22 giugno 1979, n. 338... ha stabilito la non brevettabilità dei programmi per ordinatori ed elaboratori ».

4.3. *La tutela penale del brevetto.*

La tutela penale del brevetto è prevista nel secondo comma dell'art. 474 cod. pen. che punisce chi « contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati ».

Osserva il Manzini che « codesti brevetti non possono essere che gli attestati con i quali è conceduta la privativa industriale... Ma questi attestati, trascritti sull'apposito registro e rimessi in copia a chi di ragione, sono evidentemente atti pubblici e quindi la falsità in essi commessa dovrebbe logicamente soggiacere alle sanzioni stabili-

te nell'art. 477 o 482 cod. pen. Siccome peraltro l'art. 473 li menziona specificamente, non rimane che applicare questa norma alle contraffazioni o alterazioni commesse nei detti attestati, mentre quelle sul falso documentale sono applicabili soltanto per ciò che concerne il falso ideologico (artt. 480, 483) »[88].

L'art. 88 del r.d. 29 giugno 1939 n. 1127, invece, prevede e punisce « chiunque, senza commettere falsità in segni di autenticazione, certificazione o riconoscimento, fabbrica, spaccia, espone, adopera industrialmente, introduce nello Stato oggetti in frode ad un valido brevetto di invenzione industriale ».

Infine l'art. 89 della stessa legge punisce chiunque appone, su un oggetto, parole o indicazioni non corrispondenti al vero, tendenti a far credere che l'oggetto sia protetto da brevetto.

4.4. *La tutela penale dei marchi e degli altri segni distintivi dei prodotti commerciali.*

La tutela penale dei marchi e degli altri segni distintivi dei prodotti commerciali è contenuta nell'art. 473 cod. pen. che prevede la contraffazione, l'alterazione o l'uso di segni distintivi delle opere dell'ingegno o di prodotti industriali, nell'art. 474 cod. pen. che prevede l'introduzione nello Stato e il commercio di prodotti con segni falsi e nell'art. 517 cod. pen. che prevede e punisce la vendita di prodotti industriali con segni distintivi mendaci.

Oggetto giuridico dei primi due articoli è la tutela della pubblica fede in « quei mezzi simbolici o reali di pubblico riconoscimento, che servono a contraddistinguere e a garantire la circolazione dei prodotti intellettuali o industriali (marchi o segni distintivi), ovvero a privilegiare invenzioni o speciali processi o tipi di fabbricazione (brevetti, disegni o modelli industriali) »[89].

Oggetto giuridico della norma di cui all'art. 517 è, invece, « l'interesse concernente l'ordine economico in quanto viene pregiudicato da frodi dirette agli acquirenti », la tutela della massa dei consumatori alla qualità dei prodotti in commercio e la tutela dei produttori al rispetto del corretto svolgimento dell'attività commerciale.

[88] V. MANZINI, *Trattato di diritto penale*, vol. VI, Utet, Torino, 1935.

[89] V. MANZINI, *Trattato di diritto penale*, vol. VI, p. 536, Utet, Torino, 1935. Lo stesso Autore aggiunge: « Il fatto può ledere altresì gli interessi generali dell'industria nazionale, ma in tal caso, essendosi ritenuta prevalente la lesione di codesto interesse, al titolo dell'art. 473 o 474 si sostituisce quello, aggravato per l'attentato anche alla pubblica fede, contemplato nell'art. 514 (Frodi contro le industrie nazionali) ».

Precisamente la Pretura di Milano con sentenza in data 1° giugno 1982 (est. Golia) in un caso di imitazione servile dei videogiochi Zaxxon e Frogger della ditta giapponese Sega Enterprises Ltd ha ritenuto che « il fatto denunciato, pur meritevole di tutela in altra sede, non ha rilevanza penale » e che non sono applicabili né l'art. 171 legge n. 633/1941, né gli artt. 473 e 474 cod. pen., né gli artt. 515 e 517 cod. pen., né, infine, l'art. 88 r.d. 29 giugno 1939, n. 1127.

In particolare il Pretore ha ritenuto che non fossero applicabili gli art. 473 e 474 cod. pen. in quanto « non emerge dalla denuncia che da parte delle ditte inquisite siano stati contraffatti o alterati i segni distintivi (marchio, ditta, tagione, denominazione sociale etc.) dei videogiochi della Sega. Non si lamenta, infatti, la contraffazione di alcuno di quei mezzi usati dagli operatori industriali per differenziare il proprio prodotto dagli altri analoghi e per far conoscere al consumatore da chi il prodotto è stato realizzato. Ci si duole, invece, solo del'imitazione pedissequamente servile del proprio prodotto ».

Il Pretore ha, inoltre, escluso l'applicabilità degli art. 515 e 517 del cod. pen. in quanto « nel caso in esame... all'acquirente del videogioco contraffatto non viene venduto un prodotto per origine, provenienza, qualità diverso da quello dichiarato. Gli vengono offerti e venduti prodotti firmati dalle ditte contraffatrici, proprio così come pattuito ».

Invece la Pretura di Padova con sentenza in data 15 dicembre 1983 (Est. Montini Trotti) ha ritenuto applicabile l'art. 517 cod. pen. in un caso in cui l'imputato aveva realizzato un videogioco molto simile al gioco Centipede dell'Atari e lo aveva messo in commercio con la dicitura Millepiedi.

In particolare il Pretore, dopo avere escluso l'applicabilità sia dell'art. 171 legge n. 633/1941 (... in quanto non può parlarsi della trama di un'opera cinematografica... ma... di un semplice schema di gioco...), sia dell'art. 473 cod. pen. (in quanto « ... nella specie non è ravvisabile alcuna contraffazione o alterazione di marchi o segni distintivi, poiché gli imputati non hanno tentato di imitare il nome né il simbolo della ditta denunciante...), ha ritenuto, invece, applicabile l'art. 517 cod. pen. in quanto « la riproduzione dello schema elettronico di gioco del Centipede e conseguentemente delle immagini che che ne sintetizzano le regole e la dinamica, in uso con la denominazione di Millepiedi idonea a richiamare quella del gioco distribuito dall'Atari » sono « ... modalità... per se stesse sufficienti ad indurre in inganno il compratore sull'origine o provenienza del prodotto ».

5. L'INDUZIONE IN ERRORE DI UN ELABORATORE.

5.1. *La truffa informatica.*

È ormai noto che i trasferimenti elettronici dei fondi costituiscono un nuovo modo di circolazione della ricchezza in cui lo spostamento

da un patrimonio all'altro avviene senza alcun movimento materiale di danaro o di titoli, ma soltanto attraverso istruzioni comunicate ed eseguite elettronicamente; ed è altresì noto come tali sistemi di trasferimento siano spesso oggetto di interventi dolosi diretti ad assicurarsi un ingiustificato profitto[90].

Nel nostro ordinamento non vi è alcuna norma che consideri espressamente reato il fatto di chi dolosamente abbia dato luogo ad un trasferimento elettronico ingiustificato; e vi sono molti dubbi sull'applicabilità delle norme penali in tema di reati contro il patrimonio e, in particolare, della truffa.

La difficoltà maggiore sembra costituita dal fatto che la truffa presuppone l'induzione in errore di un soggetto umano, mentre in questo caso ciò che si produce è soltanto l'errore di una macchina.

Può essere opportuno ricordare al riguardo il Manzini che, dopo avere affermato che la condotta nel reato di truffa consiste nella induzione in errore mediante artifizi o raggiri e che « è artificio, in contrapposto a raggiro, ogni astuta simulazione o dissimulazione, atta a indurre altri in errore, in modo che questo sia determinato dall'immediata percezione di una falsa apparenza materiale, positiva o negativa » aggiunge: « L'artificio, inoltre, può consistere nella manomissione o nella particolare disposizione di una cosa o di un complesso di cose, in modo da impedire al soggetto passivo, senza l'uso di straordinarie ricerche o cautele, di conoscere il vero o di avvedersi altrimenti dell'inganno »[91].

L'Autore quindi esemplifica: « Così è, ad es., nell'ipotesi dell'oste, del barbiere, ecc., che strappi abusivamente un buono dal libretto di abbonamento di un cliente, simulando in tal guisa, a danno dell'abbonato e a profitto proprio, l'avvenuta prestazione del relativo servizio. Lo stesso è nel caso di chi fa funzionare artificiosamente il tassametro d'una vettura; manomette un contatore di gas, d'acqua etc. si da ricevere più di quel che paga inducendo in errore in tal modo il fornitore; espone distributori automatici che nulla controprestino all'immissione della moneta o che altrimenti inducano in errore chi vorrebbe servirsene... »[92].

[90] Vedi tra gli altri L. PICOTTI, *La falsificazione*, p. 958; A. TRAVERSI, p. 192; G. CORRIAS LUCENTE, *Informatica e diritto penale, elementi per una comparazione con il diritto statunitense*, in questa *Rivista*, 1987, p. 541.

[91] V. MANZINI, *Trattato di diritto penale*, vol. IX, parte prima, p. 537, Utet, Torino, 1938.

[92] V. MANZINI, *op. cit.*, p. 539.

Lo stesso Autore, in nota, afferma: « Invece la truffa non è possibile da parte del doloso utente dell'apparecchio automatico. Il mettere illegittimamente in azione questi distributori non induce in errore una persona. Nel caso di distributori di cose si ha furto; in quello dei distributori di servizi si ha un fatto non punibile, non essendovi furto (neppure d'uso) perché nessuna cosa viene sottratta »[93].

Lo stesso Autore osserva ancora: « Gli artifizi o i raggiri possono bensì rivolgersi a persone indeterminate, cioè al pubblico, come nel caso di comunicazioni pubblicitarie, dell'esposizione fraudolenta di distributori automatici, di macchine da giuoco, ecc.; ma perché possa aversi il delitto di truffa è necessario che una persona determinata sia stata con tali mezzi indotta in errore »[94].

L'interpretazione così condotta del reato di truffa non dava luogo ad eccessive difficoltà nel caso dei distributori automatici per la limitata estensione all'epoca di essi e per il limitato valore economico dei beni attraverso essi distribuiti.

L'interpretazione risulta invece del tutto insoddisfacente nel caso dei trasferimenti elettronici dei fondi: questi, infatti, costituiscono ormai, e sempre più costituiranno in futuro, uno dei più importanti modi di circolazione della ricchezza; e l'esclusione del reato di truffa nella condotta di chi inganna il sistema per assicurarsi un ingiusto profitto con altrui danno risulta non solo contraria alla coscienza sociale, ma anche esiziale per la stessa funzionalità del sistema.

La dottrina ha quindi tentato di soddisfare le nuove esigenze punitive in due modi: o rinnegando il principio per cui il soggetto passivo deve necessariamente essere una persona e non una macchina ovvero confermando il principio, ma sottoponendolo ad alcuni limiti.

La prima corrente si è affermata soprattutto nella dottrina francese favorita dal fatto che in quell'ordinamento, così come nell'ordinamento belga, la norma che punisce la truffa (escroquerie) parla soltanto di *manoeuvres frauduleuses* e non richiede espressamente che queste abbiano indotto in errore una persona (art. 405 cod. pen. francese e art. 496 cod. pen. belga); e anche alcune decisioni francesi[95] e belghe[96] hanno affermato che l'utilizzazione fraudolenta di un elaboratore per la stampa di documenti attestanti crediti inesistenti può integrare gli artifici o i raggiri richiesti per la configurabi-

[93] V. MANZINI, *op cit.*, p. 540.

[94] V. MANZINI, *op. cit.*, p. 561.

[95] TIEDEMANN, *Criminalità da computer*, in *Pol. dir.*, 1984, p. 613; in Italia ritiene configurabile la truffa nel procurato malfunzionamento di una macchina U. PIOLETTI, *Truffa*, in *Noviss. Dig. it.*, App. vol. VII, Torino, 1987, p. 907.

[96] A. MANNA, *La disciplina della c.d. criminalità da computer nei paesi francofoni*, in questa *Rivista*, 1987, p. 509.

lità del reato di truffa.[97] Nella maggioranza degli altri paesi, invece, la norma che prevede la truffa richiede espressamente la induzione in errore di una persona (art. 640 cod. pen. italiano; art. 263 cod. pen. tedesco; art. 496 cod. pen. lussemburghese; art. 146 cod. pen. austriaco; art. 148 cod. pen . svizzero; capitolo 9 articolo 1 cod. pen. svedese; art. 279 cod. pen. danese; art. 386 cod. pen. greco; art. 246 cod. pen. giapponese).

In Inghilterra l'art. 15 del Theft Act 1968 parla di *obtaining property by deception* e in alcune decisioni giurisprudenziali è stata affermata la necessità dell'induzione in errore di una *human mind*[98].

Peraltro l'opinione dominante in tutti i paesi, compresa la Francia ed il Belgio, è che non vi possa essere il reato di truffa se non vi è stata l' induzione in errore di una persona determinata.

Alcuni autori, tuttavia, hanno limitato gli effetti del principio distinguendo i casi in cui l'utilità è corrisposta direttamente dall'elaboratore dai casi in cui l'utilità è corrisposta da persone fisiche che utilizzano l'elaboratore i cui dati o i cui programmi sono stati alterati dolosamente. Si pensi, ad esempio, a un mutuo concesso da funzionari di banca in base ad una situazione finanziaria erroneamente fornita da un elaboratore per il doloso intervento di un terzo. In tale caso sussisterebbe il reato di truffa; e per altri autori il reato sussisterebbe in tutti quei casi in cui vi siano persone fisiche comunque predisposte alla verifica dei dati e dell'attività svolte dall'elaboratore e che costituirebbero i soggetti passivi del reato.

In giurisprudenza è stato ad esempio affermato che sussiste il reato di truffa nel caso in cui il soggetto inserisca dati falsi in un elaboratore onde indurre in errore i funzionari dell'INPS preposti al controllo del versamento e all'esazione dei contributi previdenziali[99] ovvero gli organi di controllo di una banca[99-bis].

[97] Per un panorama di diritto comparato vedi U. SIEBER, *The international Handbook on computer crime*, J. Wiley & Sons, Chicester, 1986 p. 38 ss.

[98] Vedi *section 15 Theft Act 1968 on obtaining property by deception e section 2(1)(b) Thef Act 1978.*

[99] Trib. Roma 20 giugno 1985 (presidente e estensore Greco) in questa *Rivista*, 1986, p. 166.

In particolare il Tribunale ha affermato che configura il reato di truffa l'immissione nell'elaboratore elettronico di dati non veritieri sui pagamenti effettuati (nella fattispecie l'immissione avveniva previa falsificazione delle ricevute bancarie di pagamento).

[99-bis] Trib. Roma 14 dicembre 1985 (presidente Rotundo, estensore Cucchiari). In particolare il Tribunale ha affermato che il dipendente bancario che inserendo dati falsi nell'elaboratore rappresenta falsamente che alcuni versamenti sono avvenuti in contanti anzichè in assegni onde occultare il maggiore rischio assunto con la negoziazione di assegni prima di averne avuto confermata la copertura e di procurare il maggior lucro ai correntisti attraverso il riconoscimento della valuta liquida pone in essere artifici idonei a trarre in inganno gli organi di controllo della banca e commette il reato di truffa aggravata.

Lo stesso Tribunale ha affermato che in tale ipotesi non ricorre la figura della malversazione che postula un affidamento libero e cosciente da parte del privato di danaro o di altra cosa mobile.

Il testo della decisione è riportato in questa *Rivista*, 1988, p. 487.

È stato tuttavia osservato che le persone addette al controllo dell'attività dell'elaboratore svolgono normalmente il loro compito attraverso controlli a campione e, spesso, successivi all'esecuzione della prestazione patrimoniale e che di conseguenza viene meno in questi casi la possibilità di configurare quella « induzione di taluno in errore » essenziale per la configurazione del reato di truffa. Questa, pertanto, non è configurabile nella maggioranza dei casi; e, d'altra parte, il far dipendere la sussistenza del reato dalle modalità del controllo fa si che « la punibilità effettiva delle frodi informatiche risulterebbe ancorata ad un dato causale e occasionale »[100].

5.2. *L'uso fraudolento delle carte di credito.*

Alcuni autori hanno distinto i casi in cui l'elaboratore compie operazioni di accreditamento o, più in generale, di disposizione patrimoniale, da quelli in cui effettua consegne materiali di danaro come, ad esempio, nel caso di prelievo abusivo di danaro da uno sportello automatico come un terminale Bancomat. In questi casi la condotta di chi si impossessa abusivamente del danaro integrerebbe gli estremi del reato di furto aggravato dall'uso di un mezzo fraudolento.

Difatti la giurisprudenza belga, dopo alcune iniziali incertezze, ha considerato furto il preelievo abusivo di danaro da un cash dispenser; e ha considerato furto commesso con l'ausilio di una chiave falsa il prelievo effettuato mediante l'uso di una scheda magnetica falsa o rubata[101].

In Italia è da ricordare la decisione della Corte di Cassazione 30 gennaio 1990, n. 1162 che ha ritenuto che l'uso di una falsa carta di credito Bancomat per il prelievo di danaro da uno sportello bancario automatico integri gli estremi del reato di furto aggravato dall'uso del mezzo fraudolento[102].

La decisione ha peraltro sollevato in dottrina molte perplessità. È stato, infatti, osservato che la consegna del danaro da parte dell'elaboratore o di un terminale può essere considerata come una consegna volontaria di danaro da parte di una persona legittimata e non può pertanto integrare gli estremi della sottrazione necessaria nel reato di furto[103].

[100] G. Corrias Lucente, *Informatica e diritto penale, elementi per una comparazione con il diritto statunitense*, in questa *Rivista*, 1987, p. 543.

[101] In dottrina vedi J.P. Spreutels, *La responsabilità penale connessa ad abusi nella applicazione dell'informatica*, in questa *Rivista*, 1985, p. 131; in giurisprudenza vedi C.C. Bruxelles, 22 marzo 1973, in *Journ.*, Trib. 1974, p. 65 con nota di P. Vanderveezen. Va osservato che l'art. 467, comma 1, del codice penale belga assimila all'ipotesi di furto mediante l'utilizzazione di chiavi false, il furto commesso mediante chiavi smarrite o sottratte.

[102] È necessario osservare, peraltro, che la sussistenza degli estremi del reato di furto è stata affermata dai giudici del merito e che il ricorso per Cassazione aveva ad oggetto questioni diverse da quella della configurabilità del reato di furto e riguardava il concorso tra il reato di uso di atto falso (art. 489 cod. pen.) e il reato di furto aggravato dall'uso del mezzo fraudolento (art. 625, comma 1, n. 2 cod. pen.).

[103] G. Corrias Lucente, *Informatica e diritto penale, elementi per una arazione con il diritto statunitense*, in questa *Rivista*, 1987, p. 544.

La materia è attualmente regolata da una recente disposizione penale, l'art. 12 del d.l. 3 maggio 1991, n. 143 convertito in legge, con modificazioni, dalla legge 5 luglio 1991, n. 197 il cui testo coordinato dispone:

« Carte di credito, di pagamento e documenti che abilitano al prelievo di danaro contante.

1) Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di danaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni.

Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di danaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi ».

La norma anche se emanata in relazione alle carte di credito in genere è applicabile anche alle carte di credito a banda magnetica o a microcircuito necessarie per l'utilizzazione di uno sportello automatico di distribuzione di danaro (*cash dispenser*) o più in generale per attivare un sistema di trasferimento elettronico di fondi.

La norma è di grande importanza perché prevede e punisce un nuovo tipo di reato, l'uso indebito di una carta di credito che nel caso di strumenti informatici non era facilmente configurabile né come truffa né come furto.

Il nuovo reato può concorrere anzi con il furto mentre si ritiene che assorba il reato di truffa « in quanto si tratta di una previsione più specifica dell'induzione in errore mediante artifici o raggiri »[104].

Alcune perplessità sono state sollevate peraltro sul significato dell'espressione « non essendone titolare ». In particolare ci si è chiesti se il reato sia configurabile anche nel caso che non esista più un rapporto contrattuale valido tra l'emittente della carta e il suo destinatario e si è ritenuto che anche nel caso di risoluzione del contratto sia necessaria quantomeno una diffida per evitare « conseguenze penali gravissime e automatiche per semplici controversie civilistiche »[105].

[104] R. Borruso, *Gli aspetti legali della sicurezza nell'uso delle carte di credito e di pagamento*, in *Giust. civ.* 1992, II, 187.

[105] R. Borruso, *op. cit.*

Si è chiesto inoltre se il reato sia configurabile nel caso di uso della carta da parte del coniuge non legalmente separato o del figlio all'insaputa e presumibilmente contro la volontà del titolare; e si è ritenuto che in tal caso il reato non sarebbe configurabile a norma dell'art. 649 che esclude la punibilità dei reati contro il patrimonio in danno del coniuge non legalmente separato, di un ascendente o di un discendente o di un affine in linea retta ovvero dell'adottante o dell'adottato, di un fratello o di una sorella conviventi[106].

5.3. *L'ordine a vuoto di un trasferimento elettronico di fondi.*

Questa ipotesi si distingue nettamente da quelle in precedenza esaminate. In quelle, infatti, un terzo si introduce fraudolentemente in un sistema di trasferimenti elettronici di fondi; in questa, invece, è lo stesso titolare di una carta di credito elettronica o magnetica ad utilizzarla in modo illecito.

Tale illecito consiste generalmente nel fatto che il prelievo effettuato con l'uso della carta di credito è superiore al saldo del conto disponibile da parte del cliente ovvero al massimale prelevabile attraverso l'apparecchio.

In tali ipotesi non vi è dubbio che sussista un illecito contrattuale in quanto l'attività posta in essere è contraria a espresse clausole del contratto di ammissione al sistema. In particolare per quanto riguarda il Bancomat l'attività in questione è contraria all'art. 4, comma 2, per cui « in ogni caso il correntista è tenuto ad effettuare i prelievi entro il limite costituito dal saldo disponibile del conto ».

Non sembra invece che l'attività in questione integri gli estremi di un reato. In particolare è stato ritenuto che non sussistano gli estremi del reato di emissione di un assegno a vuoto, di truffa, di appropriazione indebita o di furto.

Per quanto riguarda infatti il furto non sussiste il necessario estremo della sottrazione in quanto l'agente ottiene il possesso delle somme attraverso la consegna materiale realizzata allo sportello e utilizzando la carta di cui è titolare; il tutto in conformità alle regole tecniche di impiego dell'apparecchio e senza alcun intervento esterno sul normale funzionamento della macchina[107]. E infatti in Francia la

[106] R. Borruso, *op. cit.*

[107] G. Corrias Lucente, *Bancomat e rilevanza penale dell'abuso da parte del correntista*, in questa *Rivista*, 1985, p. 723 ss.

Corte di Cassazione con la decisione 24 novembre 1983 ha espressamente affermato che il prelievo da distributore automatico di somme eccedenti il saldo disponibile del conto da parte del titolare di una carta magnetica si riduce ad una inosservanza contrattuale e non integra alcun illecito penalmente sanzionato[108].

Anche l'appropriazione indebita deve essere esclusa « in base alla semplice considerazione che il correntista non è entrato in possesso delle somme per alcuno dei titoli espressamente e tassativamente previsti dalla norma incriminatrice »; e ciò a meno che non si voglia configurare il potere materiale del correntista di accedere alle somme superiori al saldo come un possesso mediato; una costruzione indubbiamente artificiosa e discutibile[109].

La truffa deve essere invece esclusa non soltanto per la mancanza di induzione in errore di una persona fisica, ma, ancor prima, per la mancanza di artifizi e di raggiri. Difatti, come è stato rilevato, l'utente, per ottenere la consegna delle somme non spettantegli, non pone in essere manovre fraudolente, né dichiara falsamente di avere diritto a disponibilità non esistenti, ma si limita a formulare una mera richiesta[110].

Per quanto riguarda, infine, il reato di emissione di assegno a vuoto è stato notato che la legge « fa esclusivo e specifico riferimento all'assegno e dunque ad un oggetto affatto diverso da quello proprio dell'illecito in questione »[111].

5.4. *Legislazioni straniere.*

Come abbiamo già visto, nella maggior parte dei paesi, ad eccezione della Francia e del Belgio, la norma che prevede la truffa richiede espressamente l'induzione in errore di una persona[112]; e la dottrina e la giurisprudenza hanno escluso che il procurato malfunzionamento di una macchina possa integrare gli estremi dell'induzione in errore di una persona e costituisca quindi furto.

Ad esempio in Germania il § 263 del codice penale (Strafgesetzbuch) dispone:

« Truffa. 1) Chi, nell'intento di procurare a sé o a un terzo un vantaggio patrimoniale illecito, danneggia il patrimonio di altri, inducendolo o mantenendolo in errore mediante affermazione di circostanze false oppure mediante alterazione o dissimulazione di circostanze vere, viene punito per il reato di truffa con il carcere, oltre al

[108] La traduzione italiana della decisione è riportata in questa *Rivista*, 1985, p. 720, con nota di G. CORRIAS LUCENTE, *Bancomat e rilevanza penale dell'abuso da parte del correntista*.

[109] G. CORRIAS LUCENTE, *op. cit. ibid.*

[110] G. CORRIAS LUCENTE, *op. cit. ibid.*

[111] G. CORRIAS LUCENTE, *op. cit. ibid.*

[112] Vedi § 5, §§ 1.

quale può essere inflitta la pena pecuniaria o la perdita dei diritti civili e onorifici »[113].

L'inapplicabilità della norma alle frodi elettroniche è stata espressamente affermata dalla Commissione di esperti per la lotta contro la criminalità economica.

In particolare la Commissione ha affermato che « la fattispecie della truffa risulta spesso inapplicabile in quanto presuppone che l'offeso venga dolosamente indotto in errore. L'uomo si serve di un elaboratore per compiere determinati atti di disposizione patrimoniale (ad esempio nello sviluppo dei rendiconti delle operazioni di conto corrente, nella contabilità delle paghe del personale di un'impresa) e qualora tali dati siano oggetto di manipolazione nelle singole fasi, ricorreranno gli estremi della truffa solamente a condizione che sussista il raggiro delle persone addette al controllo delle operazioni di elaborazione elettronica... La lacuna di perseguibilità penale che si evidenzia nell'ambito della truffa deriva, detto in parole povere, dal fatto che in luogo del processo decisionale umano che conduce all'operazione di disposizione patrimoniale, in alcuni settori è subentrato l'elaboratore che non può essere dolosamente indotto in inganno, ragion per cui non ricorre un elemento essenziale della fattispecie della truffa ».

Il legislatore ha quindi emanato la legge sui reati patrimoniali in materia di informatica che ha introdotto, tra l'altro, l'art. 263a del codice penale intitolato frode informatica.

Anche in Francia, del resto, la dottrina tradizionale era nel senso dell'esclusione del reato e per questa ragione il legislatore ha emanato una apposita legge per la repressione delle truffe informatiche, la loi n. 88-19 relative à la fraude informatique.

Negli Stati Uniti si ritiene che le frodi informatiche possono integrare gli estremi dei reati federali di « wire fraud » e di « mail fraud ».

Precisamente il reato di « wire fraud » si ha quando qualcuno sia ricorso o abbia avuto intenzione di ricorrere a qualsiasi mezzo o artificio per frodare o per procurarsi danaro o altre utilità a mezzo di falsi o ingannevoli pretesti... e trasmette o fa in modo che sia trasmessa mediante telegrafo un qualsiasi scritto, firma, segno, disegno o segnale acustico allo scopo di realizzare tale mezzo o artificio...

Si ha, invece, reato di « mail fraud » quando si utilizzi il servizio postale tra i diversi stati o con l'estero per progettare o eseguire una frode.

[113] La traduzione è tratta dal Codice penale tedesco tradotto e annotato da R. Pagano, p. 153, Giuffrè, Milano, 1967.

La formulazione così ampia delle due ipotesi criminose e in particolare la mancata previsione dell'induzione in inganno di una persona come necessario estremo costitutivo del reato ha permesso facilmente alla dottrina di far rientrare in tali ipotesi le nuove figure delle frodi telematiche. In particolare la dottrina statunitense ha considerato i collegamenti telematici equivalenti, ai fini della configurabilità dei reati in questione, alle comunicazioni telegrafiche.

Ciononostante anche negli Stati Uniti sono stati presentati diversi disegni di legge allo scopo di punire con leggi particolarmente severe l'accesso abusivo ad un elaboratore appartenente a uffici federali al fine di procurare a se o ad altri danaro o altre utilità ovvero allo scopo di svolgere altra attività fraudolenta.

Il 12 ottobre 1984 sono stati emanati il Counterfeit Access Device and Computer Fraud and Abuse Act in materia di accesso abusivo ai sistemi informatici e il Credit Card Fraud Act per reprimere in modo specifico le frodi compiute con le carte di credito[114].

Quest'ultima norma prevede varie ipotesi criminose: *a*) quando si produca, si usi o si trasferisca uno o più strumenti di accesso contraffatti; *b*) quando si utilizzino uno o più strumenti di accesso non autorizzati durante il periodo di un anno e mediante tale condotta ci si procuri un ingiusto profitto pari o superiore a 1000 dollari per il periodo in questione; *c*) quando si possieda 15 o più strumenti contraffatti o non autorizzati; *d*) quando si detenga, si possieda o si traffichi con attrezzature per realizzare strumenti di accesso.

Tutti questi reati presuppongono un elemento soggettivo costituito non soltanto dalla coscienza e dalla volontà della condotta ma anche dalla consapevolezza della natura degli strumenti utilizzati o detenuti e dall'intento specifico di frodare.

La prima ipotesi è punita con una pena pecuniaria non superiore a 50.000 dollari o al doppio del valore ottenuto con il reato e/o con una pena detentiva non superiore a 15 anni; nel caso che il reato sia stato commesso dopo la reclusione per un altro reato dello stesso tipo o dopo un tentativo di commettere un reato dello stesso tipo la sanzione è costituita da una pena pecuniaria non superiore a 100.000 dollari o al doppio del valore ottenuto con il reato e/o con la pena detentiva non superiore a 20 anni.

La seconda e la terza ipotesi sono considerate meno gravi e punite con una pena minore; la quarta ipotesi, invece, è punita come la prima, ma non è previsto l'inasprimento della pena per la recidiva.

[114] Title 18 United States Code Section 1029 - Public Law 98-473 Oct. 12, 1984 - 98 Statutes at Large 2183. La legge è stata emanata insieme con il Counterfeit Access Device and Computer Fraud and Abuse Act 1984 relativa all'accesso abusivo o non autorizzato agli elaboratori.

Si tratta, come è stato osservato, di sanzioni che costituiscono un notevole inasprimento delle pene previste nel Truth in Lending Act e nell'Electronic Fund Transfer Act[115] e tuttavia molto elastiche in modo da consentire al giudice un elevato margine di discrezionalità in ordine alla misura concreta della pena e alla possibilità di applicare la sola pena pecuniaria senza un minimo edittale[116].

La norma detta inoltre una serie di definizioni dei termini usati nella legge stessa. In particolare definisce la nozione di strumento di accesso come « ogni carta, targhetta, codice, numero di conto o altri mezzi di accesso al conto che possono essere usati, da soli o insieme con altri strumenti di accesso, per ottenere danaro, beni, servizi o qualunque altra cosa di valore e che possono essere usati per attivare un trasferimento elettronico di fondi (esclusi quelli originati solamente da uno strumento cartaceo) ». L'espressione « altri mezzi di accesso al conto » è anch'essa di significato molto ampio e comprende ad esempio il numero di identificazione personale, il cosidetto P.I.N., e, in futuro, gli altri mezzi biometrici di identificazione della persona.

L'espressione « strumento di accesso contraffatto » comprende ogni strumento di accesso che sia contraffatto, fittizio, alterato o falsificato o un identificabile componente di uno strumento di accesso o di un contraffatto strumento di accesso. Per componente si intendono, invece, gli strumenti di accesso incompleti come le carte di credito in bianco, i microchips, le firme, gli ologrammi e le striscie magnetiche.

Strumento di accesso non autorizzato è ogni strumento smarrito, rubato, revocato o cancellato ovvero che è stato ottenuto con l'intento di frodare.

Infine produrre vuol dire disegnare, alterare, autenticare, duplicare o assemblare; trasferire significa, invece, vendere, affittare, prestare, distribuire, acquistare, ottenere il possesso o la detenzione.

La norma provvede anche ad istituire un Ufficio del Servizio Segreto degli Stati Uniti per accertare i reati previsti dalla legge secondo le modalità stabilite in un accordo tra il Segretario del Tesoro e il General Attorney.

115 F. MANINI, *Frodi informatiche e carte di credito magnetiche*, un'analisi del Credit Card Fraud Act, in questa *Rivista*, 1988, p. 942.

116 G. CORRIAS LUCENTE, *Informatica e dirltto penale, elementi per una comparazione con il diritto statunitense*, in questa *Rivista*, 1987, p. 551.

A livello statale, invece, è controverso anche negli Stati Uniti se siano applicabili le norme in tema di truffa alle frodi informatiche nonostante la mancanza dell'induzione in inganno di una persona. Le controversie della dottrina hanno indotto alcuni Stati ad emanare norme legislative con le quali si estendono le norme in tema di truffa alle frodi informatiche; altri Stati, invece, hanno preferito emanare disposizioni che prevedono la truffa informatica come figura autonoma di reato.

6. La tutela dei dati personali.

Nel corso degli anni sessanta, quando iniziarono a costituirsi le prime grandi banche di dati, divenne sempre più sentita l'esigenza di una normativa che tutelasse la riservatezza o *privacy* dell'individuo nei confronti della raccolta e della diffusione dei dati personali: una normativa che limitasse la possibilità di raccolta dei dati personali e attribuisse all'individuo il potere di controllare le raccolte contenenti i propri dati personali.

I primi testi legislativi in materia di banche di dati personali sono stati emanati alla fine degli anni sessanta negli Stati uniti d'America. In particolare il « Freedom of information Act » (detto Foia), approvato nel 1966, e il « Privacy Act », approvato il 31 dicembre 1974 e modificato dal « Privacy Protection Act » del 13 ottobre 1980, disciplinano le banche di dati possedute dall'amministrazione federale.

In Europa i primi testi legislativi in materia sono state le leggi di due Länder della Germania Federale, l'Assia (7 ottobre 1970) e la Baviera (12 ottobre 1970), mentre la prima legge statale è stata la legge svedese (c. d. Datalag), emanata l'11 maggio 1973 e successivamente modificata nel 1979 e nel 1982.

Altre leggi in materia sono state emanate successivamente in Germania (Bundesdatenschutzgesetz del 27 gennaio 1977), in Canada (Canadian Human Right Act - Loi canadienne sur les droits de la personne del 2 giugno 1977), in Francia (Loi relative a l'informatique, aux fichiers et aux libertés del 6 gennaio 1978), in Danimarca (Lov om private registre n. 293 e Lov om offentliche myndigheders n. 294 dell'8 giugno 1978), in Norvegia (Lov om personregistre n. 48 del 9 giugno 1978), in Austria (Datenschutzgesetz n. 565 del 18 ottobre 1978), in Lussemburgo, in Ungheria (decreto 27 gennaio 1981 n. 1 sulla tutela del segreto, del patrimonio e sulla protezione antincendio degli impianti di calcolo automatico), in Israele (Protection of Privacy Law n. 5741 del 23 febbraio 1981), in Svizzera (Directives applicables au traitement des donées personnelles dans l'administration fédérale del 16 marzo 1981), nel Regno Unito (Privacy Act n. 32 del 1984), in Finlandia (Personal Data File Act n. 471 del 3 aprile 1987 e il Personal Data File Decree n. 476 del 3 aprile 1987), in Australia (Privacy Act n. 119 del 1988), in Irlanda (Data Protection Act del 6 luglio 1988), in Giappone (The Act for Protection of Computers

Processed Personal Data held by Administration Organs n. 95 del 16 dicembre 1988), in Olanda (Data Protection Act n. 665 del 28 dicembre 1988).

Il 28 gennaio 1981 il Consiglio d'Europa emanava una « Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale » e la Commissione delle Comunità europee la Raccomandazione 29 luglio 1981 con cui raccomandava agli stati membri della Comunità di firmare entro il 1981 e di ratificare nel corso del 1982 la convenzione del Consiglio d'Europa.

L'Italia, pur essendo uno degli stati membri firmatari della convenzione, non ha sinora emanato una norma in tema di protezione di dati personali necessaria per potere ratificare la convenzione stessa.

Con decreto del Ministro di grazia e giustizia in data 5 luglio 1980 veniva affidato ad una Commissione, presieduta dall'allora Primo Presidente della Corte Suprema di Cassazione Giuseppe Mirabelli, il compito di predisporre « uno schema di disegno di legge concernente la protezione delle persone di fronte ai pericoli che ad esse possono derivare dalla raccolta e gestione dei dati personali a mezzo di sistemi automatizzati anche in relazione al flusso transfrontiera degli stessi ». Lo schema, che doveva tenere conto « dei principi che figurano in progetti di convenzioni ed in altri strumenti elaborati dal Consigli d'Europa, dalle Comunità Europee e da altri enti internazionali », veniva consegnato il 20 luglio 1982 al termine dei lavori della Commissione al Ministro di Grazia e Giustizia che lo presentava, con alcune modifiche di poco conto, al Parlamento il 5 maggio 1984.

La scadenza della nona legislatura ha comportato la decadenza sia del disegno di legge, sia degli altri progetti di iniziativa parlamentare in materia.

Nel corso della decima legislatura con decreto in data 4 febbraio 1988 il Ministro di Grazia e Giustizia istituiva un gruppo di studio con l'incarico di procedere alla revisione e all'aggiornamento del vecchio disegno di legge.

Il 30 settembre 1989 il gruppo di studio ultimava i suoi lavori e rimetteva al Ministro Giuliano Vassalli il testo definitivo della relazione e dello schema del disegno di legge concernente la disciplina delle banche di dati ad elaborazione informatica.

Nelle more dei lavori del gruppo il Parlamento approvava la legge 21 febbraio 1989, n. 98 con la quale il Presidente della Repubblica veniva autorizzato a ratificare la Convenzione di Strasburgo.

L'approvazione della legge, tuttavia, non ha sanato l'inadempienza dell'Italia nei confronti della Convenzione in quanto, in base agli artt. 4 e 22 di questa, la ratifica presuppone l'emanazione di una normativa interna conforme ai principi contenuti nella Convenzione stessa, non può essere effettuata finché non venga emanata tale normativa e, se effettuata, è del tutto inutile.

È evidente, quindi, che la legge di ratifica non ha eliminato la necessità di una disciplina delle banche di dati personali in Italia, ma,

anzi, l'ha resa più urgente così come è stato sottolineato dalle associazioni imprenditoriali. Queste, nelle audizioni compiute da parte della Commissione, hanno osservato che la mancanza di esecuzione della Convenzione porrà le imprese italiane nella impossibilità di avvalersi dell'accordo internazionale nell'attività di trasmissione e di ricezione dei dati attraverso le frontiere al momento dell'entrata in vigore dell'atto unico di integrazione europea previsto per la fine del 1992.

Al riguardo va osservato, peraltro, che la Raccomandazione della Commissione della Comunità europea prevedeva che « se entro un lasso di tempo ragionevole la firma e la ratifica della Convenzione da parte degli stati membri non avrà luogo, la Commissione si riserva di proporre al Consiglio l'adozione di un atto giuridico basato sul trattato Cee ».

In base a tale previsione il 24 settembre 1990 è stata formulata una proposta di direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali. La direttiva ha per oggetto la predisposizione di una protezione di equivalente livello in tutti gli stati membri della Comunità al fine di eliminare gli ostacoli agli scambi di dati necessari al funzionamento del mercato interno.

In materia penale ha particolare importanza l'art. 23 della direttiva così formulato:

« Art. 23. (*Sanzioni*). — Gli Stati membri prevedono nelle loro legislazioni l'applicazione di sanzioni dissuasive al fine di garantire il rispetto delle disposizioni adottate in applicazione della presente direttiva ». Infatti in tutte le normative emanate in materia vi sono disposizioni di carattere penale per le più gravi inosservanze; e così anche nei due disegni di legge italiani.

In particolare il secondo disegno di legge Mirabelli prevede tre specie di reati: l'omessa o incompleta notificazione (art. 21), la comunicazione o la diffusione illecita (art. 22) e, infine, l'omessa custodia dei dati (art. 23).

Le norme ripetono le analoghe disposizioni contenute negli artt. 23, 27 e 26 del vecchio disegno di legge. Non sono state, invece, ripetute le norme relative all'inosservanza dei provvedimenti dell'ufficio di controllo (art. 24 vecchio disegno di legge), alla raccolta illecita (art. 25), alla omissione di cancellazione o di rettifica (art. 28), alla violazione del segreto di ufficio (art. 29), alle pene accessorie (art. 30) e alle disposizioni processuali (art. 31).

In tal modo il disegno di legge ha tenuto conto della nuova funzione del Garante rispetto a quella dell'Ufficio di controllo previsto dal disegno di legge precedente ed ha assunto nel suo complesso rispetto a quest'ultimo un carattere meno criminalizzante.

In effetti le disposizioni penali del primo disegno di legge avevano suscitato numerose critiche per la loro eccessiva severità: si era parlato a questo proposito di terrorismo legislativo e non era mancato chi aveva auspicato che il sistema penale fosse limitato a sanzioni amministrative o pecuniarie.

Il secondo disegno di legge ha ritenuto, invece, « prive di efficacia, considerata la capacità finanziaria della grande maggioranza degli organismi che gestiscono le banche soggette a notificazione, sanzioni di mero contenuto patrimoniale, soprattutto se di natura amministrativa »[117]; ha quindi mantenuto la previsione di specifiche figure di reato, pur limitandole alla violazione delle norme più significative; e ciò anche in conformità all'art. 23 della proposta di direttiva della Commissione.

Attualmente, in mancanza di una normativa in tema di tutela dei dati personali, le uniche norme applicabili sono quelle contenute nella legge 1° aprile 1981, n. 121 con la quale si istituisce il Centro di elaborazione dati presso il Ministero dell' interno (artt. 6 e 8), se ne stabiliscono i limiti oggettivi (art. 7: natura ed entità dei dati e delle informazioni raccolti) e soggettivi (art. 9: accesso ai dati e alle informazioni e loro uso), le procedure per la raccolta dei dati e l'esercizio del diritto di accesso (art. 11), i controlli giudiziari, parlamentari e amministrativi (art. 10), le sanzioni nel caso che un pubblico ufficiale comunichi o faccia uso di dati e informazioni in violazione della legge o al di fuori dei fini previsti dalla stessa.

In particolare l'articolo 10 quinto comma prevede:

« Chiunque viene a conoscenza, dagli atti o nel corso di un procedimento giurisdizionale o amministrativo, dell'esistenza di dati che lo riguardano, da lui ritenuti erronei o incompleti o illegittimamente raccolti, può avanzare istanza al Tribunale penale, nel cui circondario è pendente il procedimento medesimo, perchè compia gli accertamenti necessari e ordini la cancellazione dei dati erronei o illegittimamente raccolti o l'integrazione di quelli incompleti.

Il Tribunale decide in camera di consiglio, sentito l'interessato, l'amministrazione della pubblica sicurezza e il pubblico ministero, con ordinanza da notificarsi anche al comitato parlamentare.

Avverso tale ordinanza può essere proposto ricorso per Cassazione ».

La norma è stata interpretata dalla giurisprudenza dapprima in una maniera molto restrittiva e quindi in maniera più ampia.

Difatti con sentenza 18 novembre 1985, n. 1682 la Corte di Cassazione ha dichiarato inammissibile l'istanza di cancellazione presenta-

[117] Relazione del gruppo di studio p. 23. La relazione riporta testualmente l'identico rilievo contenuto nella relazione al d.d.l. Martinazzoli.

ta da persone venute a conoscenza dei dati che le riguardavano non da atti o nel corso di un procedimento giurisdizionale o amministrativo o se l'istanza è stata presentata oltre il termine temporale di pendenza del detto procedimento[118].

Con successiva sentenza in data 8 maggio 1986, n. 1716 la stessa Corte ha invece affermato che l'interessato può proporre l'istanza in questione comunque sia venuto a conoscenza dei dati e quindi anche se li abbia conosciuti non nell'ambito di un procedimento giurisdizionale o amministrativo, ma dagli atti, vale a dire dalle più varie fonti, anche se non qualificate, come una notizia appresa in Questura o il rifiuto dell'autorità di frontiera di permettere l'espatrio con la carta di identità recante la stampigliatura « valida per l'espatrio » indipendentemente dalla pendenza di un procedimento giurisdizionale o amministrativo[119].

La Corte di Cassazione ha anche affermato — ma la decisione potrebbe sollevare qualche perplessità — che l'accertamento della legittimità del dato deve essere effettuato dal Tribunale in relazione al momento in cui il dato venne acquisito e che sono irrilevanti le vicende successive. Di conseguenza ove sia stato acquisito legittimamente un dato relativo a un fatto qualificato come reato al momento della raccolta, il Tribunale non può ordinarne la cancellazione solo perchè quel fatto sia stato depenalizzato in un momento successivo. (Cass. 5 aprile 1989, n. 1620).

Di grande importanza è anche l'art. 12 che dispone:

« (*Sanzioni*). — Il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni.

Se il fatto è commesso per colpa, la pena è della reclusione fino a sei mesi ».

Il soggetto al quale i dati o le informazioni sono comunicati non è punibile fino a quando la sua condotta si limiti al mero ricevimento

[118] La decisione è stata pubblicata sul *Foro it.*, 1986, parte II, p. 585 e sulla *Giur. it.*, 1987, parte II, p. 267.

[119] La sentenza è stata pubblicata sul *Foro it.*, 1986, parte II, p. 137 con nota di D. Carota, *Prime ipotesi applicative della normativa sulle banche dati contro la criminalità* e sulla *Giust. pen.*, 1987, parte III, p. 398 con nota di F.R. Dinacci, *Elaborazione elettronica dei dati presso il ministero dell'interno ed orientamenti giurisprudenziali in tema di procedure di correzione.*

del dato o della informazione. La giurisprudenza ha tuttavia precisato che quando la condotta dell'estraneo cessi di rappresentare un momento operativo della condotta del pubblico ufficiale ed assuma invece il concreto aspetto di una ulteriore e diversa attività propulsiva del comportamento stesso, è applicabile la disciplina del concorso eventuale nel reato prevista dall'art. 110 cod. pen. Di conseguenza è stata ritenuta la sussistenza del concorso in un caso in cui l'estraneo non si era limitato a ricevere dal pubblico ufficiale un tabulato contenente informazioni riservate, ma attraverso incontri e sollecitazioni aveva influito, sotto il profilo causale, nella determinazione del medesimo pubblico ufficiale, così partecipando, consapevolmente e con eguale intensità psicologica, alla consumazione del reato (Cass. 15 febbraio 1988, n. 2619).

Il concorso, è stato precisato — ma anche tale affermazione suscita qualche perplessità — sussiste anche quando il concorrente sia la persona alla quale le informazioni si riferiscono e i dati siano stati illegittimamente raccolti. Anche in questi casi, infatti, sussiste l'obbligo del segreto e l'interessato può fare valere i suoi diritti alla cancellazione o alla rettifica soltanto nei modi previsti dal quinto comma dell'art. 10 (Cass. 15 febbraio 1988, n. 2619)[120].

[120] Nella specie è stata ritenuta la sussistenza del concorso da parte dell'avvocato difensore.