

GIOVANNA CORRIAS LUCENTE

INFORMATICA E DIRITTO PENALE: ELEMENTI PER UNA COMPARAZIONE CON IL DIRITTO STATUNITENSE (1^a PARTE)

SOMMARIO

1^a Parte: I. CONSIDERAZIONI INTRODUTTIVE: 1. Informatica e diritto penale. — 2. Questioni terminologiche. — 3. Rilevanza dell'approccio comparatistico con particolare riguardo al sistema statunitense. — 4. Problematiche emerse per la definizione del termine elaboratore nella legislazione americana. — 5. Criteri di classificazione dei modelli comportamentali della criminalità informatica. — **II. ACCESSO ABUSIVO ED USO NON AUTORIZZATO DELL'ELABORATORE:** 1. Aspetti fenomenologici dell'accesso abusivo... — 2. (*segue*)... e dell'uso non autorizzato. — 3. La qualificazione penale di tali condotte nell'ordinamento americano. — 4. La recente legislazione in materia. — 5. L'accesso abusivo in Italia: sua irrilevanza penale. — 6. L'uso non autorizzato: sua qualificazione nell'ordinamento italiano. — **2^a Parte: III. TUTELA DEI DATI E DEI PROGRAMMI PER ELABORATORE:** 1. Apprensione e danneggiamento dei dati e dei programmi attraverso il loro supporto fisico. — 2. L'apprensione del solo contenuto. — 3. Qualificazione del fatto nella legislazione federale comune. — 4. La recente legislazione in materia. — 5. La cancellazione del contenuto dei dati e dei programmi nell'ordinamento americano. — 6. L'abusiva apprensione del contenuto di dati e programmi in relazione al sistema penale italiano. — 7. Cancellazione dei dati e dei programmi in Italia. — 8. La falsificazione dei dati. Considerazioni introduttive e disciplina dell'alterazione dei dati e dei programmi negli Stati Uniti. — 9. La falsificazione dei dati in Italia. — **IV. LE FRODI INFORMATICHE:** 1. Nozione e tecniche. — 2. Qualificazione dei fatti nell'ambito del sistema federale americano: attualità e proposte. — 3. Trattamento penale nell'ambito degli Stati americani. — 4. Rilevanza penale delle diverse fattispecie in Italia. — **V. TUTELA DELL'ELABORATORE:** 1. Il reato di danneggiamento negli Stati Uniti. — 2. Fattispecie configurabili in Italia. — **VI. BREVI CONSIDERAZIONI SULLE TECNICHE SANZIONATORIE ADOTTATE NELLA RECENTE LEGISLAZIONE STATUNITENSE IN MATERIA DI CRIMINALITÀ INFORMATICA.**

I. CONSIDERAZIONI INTRODUTTIVE.

1. *Informatica e diritto penale.*

La crescente applicazione nelle attività — economiche, sociali, politiche ed amministrative — di elaboratori automatici di dati, favori-

* Relazione presentata nell'ambito di una ricerca sulla criminalità economica in corso di svolgimento presso l'Istituto di diritto penale della Facoltà di Giurisprudenza

dell'Università di Roma « La Sapienza ». La seconda parte sarà pubblicata sul prossimo fascicolo della *Rivista*.

ta anche dalla crescita esponenziale delle loro capacità operative¹, ha posto in primo piano la necessità di analizzare e valutare il ruolo che l'elaboratore, in un rapido volger d'anni, ha assunto nei rapporti giuridici². È del resto d'immediato riscontro che l'utilizzazione di questo strumento ha introdotto nuove categorie concettuali e ha generato nuovi modelli culturali, che si differenziano da quelli impiegati come referenti tradizionali negli ordinamenti³. Offre di ciò un efficace esempio l'estensione della problematica sollevatasi nei settori del diritto civile, amministrativo, penale e processuale circa la natura ed il regime da riferire ai dati memorizzati negli elaboratori e la loro eventuale assimilazione ad entità, quali il documento⁴.

Tuttavia, anche se l'esigenza di operare un raffronto fra la nuova realtà fenomenica e la normazione esistente si pone attualmente sia rispetto al complesso dell'ordinamento giuridico che ad ogni sua singola partizione, si può rilevare che la stessa esigenza si pone in maniera differenziata e più impellente nel diritto penale, dati i principi che lo regolano. Tale ramo dell'ordinamento giuridico, infatti, appare per sua natura quello maggiormente « conservatore », poiché — integralmente informato ai principi di stretta legalità e di tipicità della fattispecie — presenta tutte le caratteristiche proprie dei sistemi chiusi, ove non operano meccanismi di adeguamento della normativa positiva alla nuova realtà fenomenica. Non vi trovano, infatti, applicazione quegli strumenti d'innovazione endogeni al sistema, come il ricorso al ragionamento analogico in funzione integrativa⁵, od esogeni ad esso, come il fattore suppletivo talora rappresentato dall'autonomia privata nel diritto civile.

L'intrinseca staticità del sistema penale comporta, dunque, la possibile inadeguatezza del suo apparato normativo a rispondere direttamente a nuove forme di aggressione ai beni o a tutelare nuove categorie di beni. Preoccupanti vuoti di tutela potrebbero, quindi, corrispondere all'attività criminosa, o *lato sensu* illecita, collegata al progresso dell'informatica, ove questa risultasse connotata d'inusuale

¹ Per le informazioni tecniche in merito alla evoluzione degli elaboratori elettronici di dati, v. L. DADDA, *Informatica ed elettronica dei calcolatori*, in *Enciclopedia del Novecento*, vol. III, Roma, 1978, p. 704 ss. Per le notizie essenziali circa il funzionamento dei sistemi di elaborazione automatica di dati cfr. E. GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984; M.G. LOSANO, *Informatica per le scienze sociali*, Torino, 1986, p. 133; P.J. DENNING, *Organizzazione e gestione dei calcolatori*, voce *Informatica*, *Enciclopedia del Novecento*, vol. III, Roma, 1978, p. 735 ss.

² Per un analitico esame della problematica si rinvia alle opere di carattere generale ed alla vasta bibliografia anche internazionale in esse citata: M.G. LOSANO, *Diritto pubblico dell'informatica*, Torino, 1986; Id., *Diritto privato dell'informatica*, Torino,

1986; A. TRAVERSI, *Informatica e diritto*, IPSOA, 1985; R. PAGANO, *Informatica e diritto*, Milano, 1986.

³ Cfr. V. FROSINI, *L'uomo artificiale*, Milano, 1986, p. 143.

⁴ Per un'ampia ricognizione di talune questioni specifiche sorte nelle diverse discipline giuridiche riguardo alla natura della documentazione informatica; R. CLARIZIA, *Informatica e conclusione del contratto*, Milano, 1985; nonché il Convegno: *Paperless Trading and the Law*, tenutosi a Bruxelles il 17-18 marzo 1986.

⁵ Non si intende in tal modo negare la legittimità al procedimento d'interpretazione evolutiva, per cui è consentito applicare la legge a fatti che, pur non essendo prevedibili all'atto della sua emanazione, possono esser compresi nel significato letterale della norma.

novità ed estensione. Come emerge da alcune compilazioni scientifiche⁶ che noverano i casi di abusi sinora verificatisi — e come verrà segnatamente esaminato nel prosieguo — l'elaboratore elettronico ha, infatti, manifestato una proteiforme capacità di partecipare al processo di realizzazione del reato (come mezzo, oggetto od « autore »⁷ dello stesso), mentre le stesse componenti del processo di elaborazione si sono dimostrate facilmente vulnerabili alle aggressioni esterne⁸.

2. Questioni terminologiche.

Gli ordinamenti nel cui ambito si è sviluppato con maggiore incisività quel fenomeno comunemente denominato « rivoluzione informatica » ne hanno, dunque, dovuto affrontare anche i riflessi penalistici. Per indicare la tematica ciascuno di essi ha adottato una propria denominazione (mentre in Italia non è ancora invalso l'uso d'un termine unico); senonché le formule coniate, per quanto simili, non sono del tutto omologhe.

Negli Stati Uniti si è a lungo discusso se fosse preferibile continuare a far uso dell'espressione per prima introdotta, l'ormai notissima « *computer crime* »⁹, oppure superare l'improprietà di questo *no-men*, sostituendolo con uno ritenuto più preciso ma, nel tempo stesso più ristretto: « *computer-related crime* »¹⁰. In entrambi i casi, secon-

⁶ Fra i diversi compendi di casistica internazionale in materia di *computer crime*: D.B. PARKER, *Crime by Computer*, New York, 1976; ID., *Fighting Computer Crime*, New York, 1983; A. BEQUAI, *Computer crime*, Lexington, 1978; U.S. DEPARTMENT OF JUSTICE, *Computer crime, Criminal Justice Resource Manual*, Washington, 1979 ed il più aggiornato R.D. NORMAN, *Computer Insecurity*, Londra, 1983. Per una documentata esposizione, talora critica, dei criteri seguiti nelle raccolte dei casi cfr. J.K. TABER, *A Survey of Computer Crimes Studies*, in 2 *Computer L.J.*, p. 275 ss (1980), il quale contesta particolarmente l'attendibilità delle fonti utilizzate in talune raccolte, in considerazione dell'esteso ricorso a materiale giornalistico piuttosto che giudiziario.

⁷ V. *infra*, note 15, 16, 17.

⁸ *Infra* capo. III.

⁹ Il frequente ricorso del termine risulta sin dai titoli delle opere: D.B. PARKER, *Crime by Computer*, cit.; ID., *Fighting Computer Crime*, cit.; A. BEQUAI, *op. cit.*; ID., *How to prevent computer crimes*, New York, 1983; inoltre il termine è utilizzato in: *White-Collar Crime: A Survey of Law*, in 18 *Am. Crim. L. Rev.*, p. 169 (1980); ID., *2nd Annual Survey of Law*, 19, *ib.*, p. 499 (1981); ID., *3d Annual Survey of Law*, 22, *ib.*, p. 494 (1984); J. BLOOMBECKER, *Computer Crime*

Update, in 7 *W. New England L. Rev.*, p. 627 (1985); L. WHARTON, *Legislative Issues in Computer Crime*, in 21 *Harvard J. on Legis.*, p. 239 (1984); S. SOKOLIK, *Computer Crime: The Need for Deterrent Legislation*, in 2 *Computer L.J.*, II, p. 353 (1980); B.J. GEORGE JR., *Contemporary Legislation Governing Computer Crimes*, in 21 *Crim. L. Bull.*, p. 389 (1985); S.H. NYCHUM, *Computer Crime, a Comment*, in 2 *Computer L.J.*, p. 2 (1980); J.K. TABER, *op. cit.*; A.M. WAGNER, *The Challenge of Computer Crime Legislation, How Should New York Respond?*, in 33 *Buffalo L. Rev.*, p. 777 (1984). Il termine è impiegato in riferimento alle singole violazioni introdotte nella legge sulla criminalità informatica dello Stato del Colorado (*Colo. Rev. Stat.*, 18-5, 5-102).

¹⁰ Nell'uso convenzionalmente invalso, tale denominazione non comprende alcuni fatti come il sabotaggio fisico od il furto delle componenti materiali dell'elaboratore. Cfr. G. THACKERAY, *Computer-related Crime: and Outline*, in *Jurimetrics*, p. 300 (1985); L. MENNELLY, *Computer-related Crime in U.S., Canada and England: New Laws for Old Offences*, in 8 *B.C. Int'l Comp. L. Rev.*, p. 551 (1985). L'espressione recepita nelle leggi statunitensi perde di specificità, designando anche fatti di attentato o sottrazione dell'elaboratore. v. ad esempio, il preambolo

do la caratteristica ottica pragmatica del mondo anglosassone, la definizione fa riferimento al fatto lesivo ed al mezzo (od oggetto) dell'azione.

In Germania si è, invece, prescelta una prospettiva soggettivistica, ed è invalso l'uso del termine « *Computer-Kriminalität* »¹¹, che accentua l'impostazione socio-criminologica propria dello studio sull'argomento. In Francia è stato un riferimento d'ordine sistematico a prevalere e generalmente s'indica la materia di studio come « *droit pénal de l'informatique* »¹².

Le differenze terminologiche che si possono immediatamente riscontrare dipendono, innanzitutto, dallo scorcio prospettico (sostanziale, criminologico o sistematico) adottato per denominare i nuovi fenomeni; appaiono, però, di maggior rilievo le conseguenze di ordine sostanziale dipendenti dalla scelta del secondo termine che partecipa alla definizione (*computer* od *informatica*) da cui deriva una diversa estensione della materia di studio. Ciò risulta evidente considerando che con l'espressione « *informatica* »¹³ si designa la disciplina scientifica che ha ad oggetto il trattamento automatico dei dati, di cui l'elaboratore non rappresenta che una componente. Tanto che gli abusi connessi all'elaboratore consisterebbero, secondo una classificazione operata sulla base di osservazioni empiriche¹⁴, esclusivamente negli illeciti commessi: a) a mezzo del *computer*¹⁵; b) a danno del *computer*¹⁶; c) « dal *computer* »¹⁷. Essi costituirebbero perciò solo un

in Fla Stat Ann 81502 (2); Md Crim. Law Code Ann., par. 146.

Come rileva M.D. SCOTT, *Computer Law*, New York, 1984, par. 8.2 il termine è stato per la prima volta introdotto nel rapporto del GAO (*General Accounting Office*), *Federal Programs*, 1979, 1.

¹¹ U. SIEBER, *Computer Kriminalität und Strafrecht*, Köln, 1980; E.J. LAMPE, *Die Strafrechtliche Behandlung der sog. Computer-Kriminalität*, GA, 1975; R.A.H. VON ZUR-MUHLEN, *Computer-Kriminalität. Gefahren und Abwehr*, Berlin, 1973.

¹² R. GASSIN, *Le droit pénal de l'informatique*, in *D.*, *Chr.*, 1986, p. 35; AA.VV., *Emergence du droit de l'informatique*, Paris, 1983, p. 149 (per la parte penale); P. SARGOS, M. MASSE, *Le droit pénal spécial né de l'informatique*, in *Informatique et droit pénal*, Paris, 1983, p. 22. Deve comunque rilevarsi che recentemente è stato impiegato il termine « *fraude informatique* », come omologo di *computer crime* cfr. *Droit de l'informatique*, 1986, in *Dossier: Fraude Informatique*.

¹³ M.G. LOSANO, *Informatica per le scienze sociali*, cit., p. 143; voce *Informatica*, *Dizionario Enciclopedico Treccani*, vol. III, Roma, 1970, p. 472. Una ricostruzione delle origini, nonché dei significati attribuiti al termine *informatica* è effettuata da M.G. LOSANO, *op. ult. cit.*, p. 337 ss.

¹⁴ Cfr. D.B. PARKER, *Crime by Computer*, cit., p. 17; *Id.*, *Fighting...*, cit., p. 173; S. SCHØLBERG, *Computer and Penal Legislation*, Oslo, 1983, p. 5 ritiene di dover far esclusivo riferimento alle due classi degli illeciti commessi a danno e per mezzo del *computer*.

¹⁵ Si tratterebbe degli illeciti in cui l'elaboratore assume il ruolo di strumento attivo: le frodi informatiche, la cancellazione o la riproduzione dei dati ordinate attraverso i sistemi elettronici. R. GASSIN, *op. cit.*, p. 40 include in tal novero anche gli illeciti in cui l'elaboratore funge da strumento passivo.

¹⁶ Fra questi illeciti di ricomprendono le varie ipotesi di sabotaggio dell'elaboratore ed anche il c.d. « furto di tempo », per cui si veda più dettagliatamente *infra*, cap. III.

¹⁷ A quest'espressione sono ricondotti due distinti significati. Secondo D.B. PARKER (v. da ultimo in: *Fighting*, cit., p. 17) con tale locuzione si dovrebbero designare i casi in cui l'ambiente di elaborazione dati agevoli, o divenga l'occasione per perpetrare un illecito.

In un diverso senso l'espressione verrebbe utilizzata in maniera impropria, per quanto suggestiva, per indicare i fatti di natura colposa, conseguenti all'erronea manutenzione o programmazione dell'elaboratore. Quale tipico esempio viene usualmente proposto il caso

settore degli abusi resi possibili dalla nuova tecnologia, i quali parimenti possono avere ad oggetto altre componenti dei processi informatici, come i dati od i programmi, indipendentemente dal loro attuale inserimento nell'elaboratore. Le formule « reati informatici » e « criminalità informatica » appaiono, quindi, più comprensive, in quanto, indicando sinteticamente l'intero settore scientifico cui il *computer* appartiene, non circoscrivono l'attenzione a quei soli fatti in cui partecipa direttamente lo strumento elaboratore.

In Italia ove, come si è rilevato, non è ancora invalso l'uso di un unico termine, e le proposte avanzate sinora spesso consistono in libere trasposizioni dei termini stranieri, si è recentemente mostrata una certa preferenza per il termine « reati informatici »¹⁸. Non mostra, invece, alcun particolare pregio il tentativo d'introdurre il termine « reati elettronici »¹⁹ suscettivo di rendersi inadeguato ad indicare l'intera materia. Infatti, se l'elettronica è la struttura tecnica attualmente d'impiego più esteso negli elaboratori di dati, essa tuttavia non è l'unica tecnica impiegata, ma sono già in uso elaboratori ottici, chimici e magnetici²⁰.

Altri interessanti spunti per la precisazione della materia di studio si possono ricavare dall'analisi del significato riferito all'altro termine della definizione (reato, diritto penale o *crime*). Va in proposito osservato che è invalsa ormai una sorta di convenzione secondo cui questi termini non vengono adoperati, rispetto all'argomento specifico, nel significato tecnico-giuridico loro proprio, ma per le esigenze peculiari della materia, essi sono invece utilizzati fuori da ogni prospettiva formalistica. Sicché, comunemente, non s'intendono per

della collisione aerea dovuta ad un errore dell'elaboratore che governa il traffico aereo-portuale (cfr. a quest'ultimo riguardo, C. SARZANA, *Sviluppo tecnologico e criminalità, in Informatica ed evoluzione economica dell'attività giuridica*, Firenze, 1985, p. 159; S.H. NYCUM, *Legal Problems of Computer Abuse*, in 3 *Wash. U.L.Q.*, p. 527 (1977), part. p. 535 constata (il prevedibile) orientamento delle Corti Americane di riferire agli addetti alla programmazione, manutenzione o controllo del computer la responsabilità dei relativi errori dannosi. Recentemente D.B. PARKER, *op. loc. cit.*; M.D. SCOTT, *op. cit.*, par. 8.11; hanno rilevato che l'elaboratore può svolgere anche il ruolo di simbolo, nell'ambito di taluni reati; si è con ciò rilevato che le minacce o le estorsioni aventi ad oggetto il sabotaggio fisico dell'elaboratore o la cancellazione dei dati o dei programmi dispiegano un concreto effetto intimidatorio nei confronti delle vittime (dato il valore delle funzioni svolte e dei materiali impiegati nei processi informatici).

¹⁸ Così C. SARZANA, *Note sul diritto dell'informatica*, in *Giust. pen.*, 1984, I, 21; L. PICOTTI, *La falsificazione dei dati informatici*, in questa *Rivista*, 1985, p. 939, p. 940, nota 4, che, pur ritenendo sostanzialmente equivalenti le espressioni, considera più appropriate quelle contenenti il termine informatica a designare l'intera materia.

¹⁹ L. TRIA, *Osservazioni in tema di reati elettronici*, in *Arch. pen.*, 1984, p. 283 definisce come tali « le fattispecie criminose per la cui sussistenza è necessaria l'utilizzazione degli strumenti elettronici propri del sistema bancario » (part. p. 286).

²⁰ Per una critica a tale denominazione si veda anche L. PICOTTI, *op. loc. cit.*. Riguardo alle strutture tecniche utilizzate negli elaboratori, cfr., J.B. TOMPKINS e L.A. MAR, *An Analysis of 1984 Federal Computer Provisions*, in *L. & Techn.*, p. 1, part. p. 8 (1985), ed in generale le questioni sorte per la corretta definizione del termine *computer* nella legislazione americana, sintetizzate *infra*.

« reati informatici » solo i fatti penalmente perseguibili nell'ordinamento, ma anche quei fatti che comunque appaiano socialmente pericolosi o dannosi²¹, ovvero, in un senso più ristretto e forse parzialmente più corretto, quei fatti, di volta in volta, ritenuti meritevoli di sanzione penale²². Il termine reato (o *crime* o diritto penale) viene dunque assunto in un significato quantomeno improprio, cui tuttavia difficilmente potrà rinunciarsi, sia perché nel suo impiego è implicita un'istanza di tutela futura, sia per la maggior suggestione e semplicità che presenta rispetto a formule più appropriate quali « abusi connessi all'informatica », od all'utilizzazione dell'elaboratore.

L'indagine terminologica consente pertanto d'individuare quale sia la tendenza propria degli studi sull'argomento: essi concernono non solo i fatti attualmente previsti come reato dall'ordinamento, ma anche quei fatti che, pur non rientrando per la loro novità in una fattispecie penale posta, tuttavia, in considerazione della struttura e/o dei connotati che presentano, si auspica che presto vi vengano ricompresi. È una ricerca, dunque, che oscilla fra valutazioni di diritto positivo e *de iure condendo*, ed in quest'ultimo ambito è tesa a discernere i fatti che necessitano d'essere penalmente sanzionati, o si ritiene opportuno che lo siano.

3. *Rilevanza dell'approccio comparatistico con particolare riguardo al sistema statunitense.*

Il delinearsi di questioni penali connesse all'informatica ha in particolare evidenziato l'opportunità di un'analisi comparatistica, che consenta d'individuare tempestivamente quali siano i diversi comportamenti illeciti, di approfondirne la fisionomia e valutarne la rilevanza penale, alla luce del diritto vigente o di considerazioni di politica criminale.

Lo studio dell'esperienza americana si presenta particolarmente proficuo per soddisfare quest'esigenza. La ragione di ciò risiede manifestamente nel fatto che la società statunitense ha iniziato con grande anticipo, rispetto ai paesi europei, i processi d'informatizzazione e può essere considerata più evoluta in tale settore. Conseguentemente i fenomeni di rilevanza penale connessi all'informatica si sono là manifestati da tempo e sono stati oggetto d'indagine, analisi e classificazione quando ancora in Italia non si era sollevata alcuna questione in argomento. L'esperienza statunitense può dunque costituire una sorta di « periscopio sul futuro » con il quale distinguere i diversi modelli comportamentali fatti propri dalla criminalità informatica prima che si riproducano nel nostro ordinamento.

²¹ In tal senso K. TIEDEMANN, *Criminalità da computer*, in *Pol. dir.*, 1984, p. 613, part. p. 614.

²² Molto chiaramente: L. PICOTTI, *op. cit.*, p. 941 nota 6; C. SARZANA, *Informatica e diritto penale. Problemi, prospettive ed aree*

di ricerca, Relazione al Convegno: *La Criminalità informatica, prevenzione e repressione*, organizzato dal CED, Roma 4-6 dicembre 1986, p. 3, segnala come tale definizione si inserisca in una prospettiva criminologica.

Va però sottolineato che l'importanza dell'esperienza statunitense non si riduce all'aspetto criminologico della materia, ma ne investe il settore più propriamente tecnico-giuridico. Come si esaminerà nel prosieguo, all'avanzamento tecnologico negli U.S.A. è corrisposta una concreta tendenza alla legiferazione della materia dei *computer crimes*²³; e sia a livello federale che a livello statale si è proceduto alla creazione di nuove fattispecie di reato, od all'adeguamento legislativo di quelle esistenti. I dati normativi così ricavabili possono offrire preziose indicazioni — per quanto sia indubbio che lo studio rivolto al sistema di leggi adottate in un'altra nazione non debba indulgere in irriflessive assimilazioni, che prescindano dalle rilevanti differenze esistenti fra gli ordinamenti — e nel contempo segnalare gli ulteriori problemi che si possono presentare allo stadio normativo della materia.

Senonché, oltre queste motivazioni comuni ad ogni studio comparatistico, nel settore della criminalità informatica se ne potrebbe individuare un'altra, peculiare, correlata alle potenzialità tecniche ed alla rilevanza internazionale dei mezzi attualmente a disposizione, come ad esempio i sistemi di elaboratori che operano in connessione tra i diversi stati, consentendo il flusso dei dati oltrefrontiera (*transborder data flow*) e la conclusione immediata (in *real time*) di operazioni complesse²⁴. D'importanza rilevante è in questo ambito la rete interbancaria, che collega gli istituti di credito di diversi paesi, attraverso la quale si possono effettuare trasferimenti elettronici di fondi ed altre operazioni bancarie con l'estero²⁵. La possibilità introdotta da questi sistemi, che un comportamento si svolga quasi contemporaneamente in diversi stati, ha indotto alcuni studiosi a sollecitare l'introduzione di una comune regolamentazione, così da disciplinare in maniera unitaria, le diverse questioni processuali e sostanziali attinenti tali reti di elaborazione e gli illeciti mediante esse perpetrati²⁶, ed evitare che si costituiscano i c.d. « paradisi informatici » ove sia

²³ Cfr. la parte seconda per un'analisi particolareggiata. In questa sede pare sufficiente segnalare che il Congresso Federale ha emesso nel 1984 una legge: il *Counterfeit Access Device and Computer Fraud Act*, per reprimere alcuni abusi connessi all'informatica; sono stati, inoltre, proposti diversi progetti di legge che concernono altri illeciti. Nel contempo più della metà degli Stati americani ha emesso leggi specificamente rivolte alla criminalità informatica; un elenco delle medesime è riportato da G. THACKERAY, *op. cit.*, p. 300; e riprodotto da M.G. LOSANO, *Il diritto privato*, cit., p. 149; un prospetto di agevole consultazione è contenuto in T.H. SOMA, P.J. SMITH e R.D. SPRAGUE, *Legal Analysis of Electronic Bulletin Board Activities*, in 7 *W. New England L. Rev.*, p. 571 (1985).

²⁴ M.G. LOSANO, *Il diritto pubblico*, cit., p. 11.

²⁵ La principale delle reti è la c.d. SWIFT, sul punto si v. L. PATRIA, *Trasferimento elettronico di fondi*, Atti del convegno: *Aspetti economici, giuridici ed organizzativi nelle esperienze estere e nella realtà italiana*, Piacenza, 12 novembre 1983; S. MACCARONE, *Il trasferimento elettronico dei fondi nel diritto italiano*, in questa *Rivista*, 1985, p. 605; P. NUVOLONE, *La trasmissione elettronica di fondi e la tutela dell'utente*, ib., 1985, p. 593, part. p. 596; D.B. PARKER, *Fighting*, *op. cit.*, p. 267; P. DI BLASI, *I rischi informatici dell'automazione delle banche*, p. 4 s., *Relazione Convegno CED*, cit.

²⁶ Le proposte sono state avanzate da studiosi europei: P. CATALA, *Emergence du droit de l'informatique*, cit., p. 5; U. SIEBER, *De la nécessité d'une législation internationale contre la fraude informatique*, in *Dr. inf.*, 1985, *Dossier*, p. 4; ID., *The International Handbook on Computer Crime*, New York

preclusa la persecuzione penale del reo. Tali finalità potrebbero venir raggiunte mediante la predisposizione d'una specifica convenzione, che obblighi gli Stati aderenti all'emanazione di normative in materia, il cui contenuto sia stabilito, nelle linee generali, dalla medesima convenzione²⁷.

Se tale proposta non ha avuto sinora seguito ed appare, comunque, di difficile realizzazione, tuttavia è interessante cogliere attraverso essa l'anticipazione d'un ordine di problemi, che potrebbero venirsi a porre nei singoli ordinamenti, circa le questioni del *tempus e locus commissi delicti*, in relazione alle dimensioni spaziali e temporali degli illeciti commessi mediante le reti internazionali di elaborazione di dati.

4. *Problematiche emerse per la definizione del termine elaboratore nella legislazione americana.*

Passando all'esame nel dettaglio delle scelte operate nell'ordinamento americano, si può constatare che i legislatori statunitensi sono stati a lungo impegnati in una questione solo apparentemente di ordine definitorio: precisare il significato da attribuirsi al termine *computer*, sul quale s'impernavano le diverse fattispecie di reato introdotte²⁸. Il problema si è rilevato particolarmente complesso, sia perché alla sua soluzione non veniva in soccorso l'apporto dei tecnici (che avevano coniato definizioni vaghe o tautologiche)²⁹, sia perché occorre una definizione specificamente finalizzata alla materia. Inoltre, negli anni in cui la normativa statunitense veniva emessa, la

1986, p. 114; B. DE SCHUTTER, *Trend in the Fight Against Computer-related Delinquency*, p. 5, Relazione Convegno CED, cit.

S. SCHØLBERG, *op. cit.*, p. 45, ha proposto un modello dettagliato per la legiferazione dei più comuni reati informatici. Il Consiglio di Europa ha istituito da tempo una Commissione di esperti per vagliare la praticabilità e i termini contenutistici d'una possibile omologazione del diritto penale dei singoli Stati europei in materia.

²⁷ Cfr. S. SCHØLBERG, *op. loc. cit.* Un'acuta analisi delle funzioni degli strumenti convenzionali per la repressione della criminalità di dimensioni internazionali è condotta da C. PEDRAZZI, *Il ravvicinamento delle legislazioni penali nell'ambito delle legislazioni europee*, in *Prospettive per un diritto penale europeo*, Atti IV convegno di diritto penale, Bressanone, 1967, Padova, 1968, p. 457; e da S. GLASER, *Le principe de la suprématie du droit pénal européen*, *ib.*, p. 387. Tali strumenti si presentano come il mezzo più efficace e sperimentato per ottenere una regola-

mentazione legislativa unitaria per fatti di rilevanza internazionale, nel rispetto della sovranità statale dei singoli aderenti. Per un'analisi di talune problematiche inerenti al tema cfr. C. SARZANA, *Informatica*, Relazione CED, cit., p. 4.

²⁸ Le disposizioni sono riportate nella seconda parte, in corrispondenza alle fattispecie prese di volta in volta in esame. Un analogo problema definitorio in relazione alla nuova tecnologia, si è posto nella Germania Federale, ove si è dovuta inserire nella 2 WikG del 15 maggio 1986 la definizione del termine « dato », riferendolo a quelli « memorizzati elettronicamente, magneticamente od in altro modo intelligibile dall'uomo, ovvero che vengono trasmessi a distanza » (par. 202, co. III StGB), cfr. al riguardo L. PICOTTI, *La nuova normativa in tema di criminalità da computer nella Repubblica Federale tedesca*, p. 5, in *corsi di pubblicazione*.

²⁹ Per la valutazione della vaghezza delle definizioni non giuridiche del termine *computer*, cfr. J. TOMPKINS e L.A. MAR, *op. cit.*, p. 10.

tecnologia degli elaboratori era (come del resto tuttora) in continua e rapida evoluzione, con una costante modificazione delle caratteristiche strutturali e funzionali delle sue componenti. Queste venivano ridotte nelle dimensioni e si avevano così gli *home* e i *personal computer*³⁰, le piccole agendine tascabili elettroniche, per più versi dissimili dai grandi centri di elaborazione dati cui si aveva inizialmente riguardo.

L'ampiezza della problematica al riguardo sorta emerge con chiarezza dal confronto delle definizioni contenute in alcune leggi statali, nella legge federale e nei diversi progetti legislativi proposti.

Una delle prime definizioni è inserita nel progetto di legge (contrassegnato dal n. S.240) presentato al Senato nel 1979 dal sen. Abraham Ribicoff e tuttora non approvato. Ai fini delle incriminazioni previste nel testo il *computer* viene definito come « un dispositivo elettronico che svolge funzioni logiche, aritmetiche, o di memoria attraverso la manipolazione d'impulsi elettronici o magnetici »³¹, definizioni d'identico contenuto sono state riprodotte nelle leggi emanate da diversi stati in materia di *computer crimes*³². Si possono tuttavia rilevare alcune insufficienze negli aspetti salienti della definizione riportata, ed in particolare nell'identificazione delle caratteristiche strutturali e funzionali dell'elaboratore. Per il primo profilo, pare opportuno evidenziare che la sua portata resta circoscritta ai soli dispositivi elettronici (che come si è già considerato rappresentano l'attuale maggioranza degli elaboratori) ne restano però esclusi i macchinari costruiti con l'impiego di altre tecniche (ottica, magnetica, ecc.) che allo stato hanno un certo impiego, seppur non esteso³³. Non è fuor di luogo, dunque, la preoccupazione che l'inserzione di questa definizione in un testo legislativo sia a sua volta suscettibile d'ingenerare lacune normative, valendo ad escludere, dalla sfera di operatività delle disposizioni penali, gli strumenti che si avvalgano di tecniche diverse da quella elettronica. Per l'aspetto funzionale essa è, invece, troppo generica, in quanto vi si possono far rientrare congegni come le macchine da scrivere elettroniche, i *computers* tascabili nonché una miriade di piccoli dispositivi capaci di svolgere, anche se in proporzione ridotta o limitata, le funzioni indicate³⁴.

³⁰ Sulle caratteristiche dei *personal computers*, nelle linee essenziali, M.G. LOSANO, *Informatica per le scienze sociali*, cit., p. 155 ss.

³¹ S. 240.1028 (c)2, il testo è riportato in 2 *Computer L.J.*, p. 723 (1980). Per tale parte il progetto riproduce integralmente il contenuto dell'altra proposta di legge presentata al Senato dal medesimo sen. A. Ribicoff, nel 1977, S. 1766.

³² Ariz. Rev. Stat. Anno, par. 13-2301 E.2; Colo. Rev. Stat., par. 18-5 5-101 (2); Mich. Stat. Ann., par. 28. 529 (2). 2; N.M. Stat. Ann., par. 30-16A-2B; R.I. Gen. Laws,

par. 11-52-1 (B); M. Crim. Law Code Ann., par. 27-168 (c).

³³ Così L. WHARTON, *op. cit.*, p. 244; A.M. WAGNER, *op. cit.*, p. 802.

³⁴ Critiche in tal senso sono avanzate dagli stessi autori citati alla nota precedente: A.M. WAGNER, *op. cit.*, p. 676; L. WHARTON, *op. cit.*, p. 239-243; il quale ultimo (con riferimento all'identica formulazione contenuta nel progetto H.R. 1092, presentato dal deputato Nelson) contesta inoltre la « inutile estensività » della definizione ritenendo che essa possa designare persino i sistemi organici capaci di svolgere le funzioni indicate.

Questa definizione è, quindi, da un lato suscettiva d'esser superata dall'avanzamento della tecnologia (qualora si avvalga di tecniche diverse dall'elettronica) e dall'altro amplifica la portata delle leggi penali includendovi anche congegni di estrema semplicità.

Un'altra formula definitoria, adottata nelle disposizioni legislative di altri stati, considera il *computer*: « un dispositivo automatico internamente programmato che svolge l'elaborazione di dati »³⁵. Oltre il pregio della sintesi, questa definizione ha quello di una maggiore comprensività, dovuto alla sostituzione del riferimento alla tecnologia elettronica con il diverso concetto di « automatico », cui possono esser ricondotti elaboratori che si avvalgano di diverse tecniche. Ciononostante anche questa formula definitoria, come la precedente, ha il difetto d'esser troppo estensiva e di non introdurre correttivi all'individuazione generica degli aspetti funzionali del *computer*³⁶.

Nell'ambito dei diversi testi legislativi emanati in materia di criminalità informatica — di cui si sono citati i più significativi — la scelta operata in argomento dal Parlamento federale statunitense appare sinora la più completa, probabilmente perché, ultima in ragione di tempo, ha certamente potuto trar vantaggio dalle precedenti esperienze ed anche dalla conoscenza delle più recenti innovazioni tecniche. Tale definizione, contenuta nel *Counterfeit Access Device and Computer Fraud Act* approvato dal Congresso nel 1984, supera alcune delle difficoltà in precedenza segnalate e tiene conto di ogni « dispositivo di elaborazione dati elettronico, magnetico, ottico, elettrochimico e elettromagnetico, o comunque ogni dispositivo di elaborazione di dati ad alta velocità, incluse le apparecchiature per l'archiviazione dei dati o le comunicazioni, operanti in connessione con tale dispositivo », precisando che « il termine non comprende le macchine da scrivere, o le macchine compositrici, i calcolatori portatili e simili congegni »³⁷. Il Congresso americano ha inteso così adottare una definizione al massimo esaustiva applicando due criteri: per quello strutturale si sono precisate, sia partitamente che genericamente, le tecniche di cui si vale lo strumento e per quello funzionale si sono indicate genericamente (elaborazione dati) le operazioni che l'elaboratore è in grado di svolgere³⁸. Tale definizione si presta per la sua genericità ad essere adattata — nel vasto ambito delle strutture techni-

³⁵ Fla. Stat. Ann., par. 815.03 (2); N.C. Gen. Stat., par. 14-453 (2); Utah Crim. Code, par. 76-6-702 (2); Minn. Stat. Ann., par. 609.861.4; Mo. Ann. Stat., par. 1.2; S.D. Codified Laws Ann., par. 43.2.2 (1); l'Illinois ha invece adottato una definizione analoga ma diversamente espressa, Ill. Crim. Code sec. 16-9 (a). 1.

³⁶ Così A.M. WAGNER, *op. cit.*, p. 802; L. WHARTON, *op. cit.*, p. 243.

³⁷ 18 USC par. 1030, J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 9, rilevano che la defi-

nizione è stata ottenuta combinando le proposte formulate nel progetto H.R. 1092 (nel quale non erano previste espresse eccezioni per determinati congegni), e, nel progetto S. 2940 (presentato dall'*U.S. Department of Justice*) nel quale era, invece, prevista l'esclusione degli *home e personal computers*, purché non utilizzati in connessione con un altro elaboratore.

³⁸ Al riguardo v. l'esteso commento di J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 6.

che indicate — anche ad elaboratori più sofisticati di quelli che attualmente vengono prodotti od impiegati. In tal senso presenta una certa duttilità, connotato di grande importanza in questo campo, poiché concorre ad evitare che la legislazione speciale in materia informatica divenga obsoleta allo stesso passo dei materiali cui faceva riferimento.

Ma un altro merito può esserle ricondotto: quello di aver convenzionalmente circoscritto la portata del termine *computer*. Come si è considerato la preoccupazione di render esaustiva la definizione comporta il rischio che essa nella sua comprensività includa anche dispositivi di elaborazione dati di limitate capacità, ma di uso ormai esteso, i quali non meritano una tutela pari a quella offerta dalla legislazione statunitense agli elaboratori. Il segnalato rischio è stato superato in parte dalla legge federale, escludendo dalla tutela specificamente approntata per gli elaboratori automatici di dati, le macchine da scrivere e, con una « formulazione aperta », altri dispositivi analoghi³⁹, le cui caratteristiche appaiono individuabili in limitate funzioni esecutive, spettro ristretto di attività e ridotta potenzialità di memoria.

Recentemente sono state formulate alcune critiche anche verso la definizione contenuta nella legge federale del 1984. Tali obiezioni si fondano sulla considerazione che le capacità operative degli strumenti espressamente esclusi dalla legge federale potranno essere in futuro ampliate sino a renderle pari a quelle proprie degli elaboratori attualmente compresi nella normativa, tanto da far risultare inopportuna ed ingiustificata la limitazione così operata⁴⁰.

Un certo interesse è stato per tali ragioni rivolto al più recente fra i progetti di legge proposti in materia di criminalità informatica nello Stato di New York⁴¹, nel quale, con un sensibile distacco dalle formulazioni sinora adottate, si è precisato che le norme penali si riferiscono ai soli *computers* impiegati negli affari, nell'amministrazione o nell'educazione⁴². Il tentativo così effettuato di circoscrivere la portata delle disposizioni legislative non pare sostenuto, però, dall'individuazione di un corretto criterio di discriminazione del lecito: si può infatti considerare che, se la normativa risulta in parte giustificata in quanto nei settori di attività individuati dovrebbero effettivamente verificarsi i fatti di dimensioni più gravi, è anche vero che attraverso essa verrebbero sottoposti a sanzione penale pure fatti — come l'uso d'una macchina da scrivere — che non paiono rivestiti di pericolosità maggiore solo perché ineriscono alle attività indicate.

³⁹ *Op. ult. cit.*, p. 10.

⁴⁰ Critiche in tal senso sono avanzate da L. WHARTON, *op. cit.*, p. 244.

⁴¹ Ampie notizie sui diversi progetti di legge presentati per lo Stato di New York (e a quanto consta, non ancora approvati) sono offerte da A.M. WAGNER, *op. cit.*, p. 801 ss.;

E.A. GLYNN, *Computer Abuse: The Emerging Crime and the Need for Legislation*, in 12 *Fordham Urb. L.J.*, p. 73 (1984), part. p. 94 ss.

⁴² Tale definizione è inserita nel progetto di legge S. 494; in merito ad essa v. E.A. GLYNN, *op. cit.*, p. 98 ss.

In ultima analisi, una definizione del termine « elaboratore » che soddisfi compiutamente le molteplici esigenze del diritto penale non appare ancora coniata, per quanto l'esame di quelle adottate negli Stati Uniti offra indicazioni utili. Talune delle questioni sollevate e delle soluzioni prospettate per quel sistema, prestano, infatti, interesse anche per ordinamenti non adusi a cristallizzare normativamente le definizioni di tutti i termini legislativi, come invece avviene in America. Le considerazioni dianzi effettuate rendono infatti palese il rischio di eccessiva criminalizzazione che può conseguire all'inserzione del termine « elaboratore » in un testo legislativo, senza una limitazione della sua portata o, per altro verso, dell'operatività della norma.

5. *Criteri di classificazione dei modelli comportamentali della criminalità informatica.*

Dopo tali considerazioni di ordine generale è possibile esaminare le questioni attinenti le singole fattispecie concrete individuate dalle ricerche scientifiche statunitensi, la loro penale qualificazione nell'ambito dell'ordinamento americano — alla luce della recente legislazione in materia di *computer crimes* ovvero della preesistente normativa —; nonché effettuare un primo tentativo di qualificazione di tali fattispecie nell'ambito del sistema penale italiano.

Prima di procedere oltre, converrà tuttavia formulare qualche breve precisazione di ordine metodologico. Nella partizione delle diverse ipotesi d'illeciti è parso di dover prescindere da quelle classificazioni adottate da parte della dottrina americana, che usa distinguere i *computer crimes* in quattro figure (vandalismo; furti o truffe aventi ad oggetto informazioni o programmi; frodi finanziarie; furto di servizi)⁴³; ovvero in dodici figure (furto di proprietà, dati o servizi; accesso abusivo; falsificazione dei dati; fatti colposi con conseguenze sulle persone; estorsioni; violazioni della riservatezza; sabotaggio; furto di materiali; falsificazione di elaborati; furto di tessere per ATM; violazione del segreto relativo al numero delle carte magnetiche)⁴⁴ onde evitare, per quanto possibile, inutili duplicazioni nel trattare le problematiche che si propongono in maniera analoga per più d'un argomento. Si è, invece, preferito individuare alcune ipotesi e sistemarle, per comodità di trattazione, secondo criteri di duplice natura: fondati ora sul riferimento alla condotta aggressiva (accesso abusivo, uso non autorizzato, frodi informatiche) ora al bene leso (tutela dei dati e dei programmi, tutela dell'elaboratore). Tale impostazione è apparsa più consona anche in considerazione della com-

⁴³ *White-Collar Crime, A Survey of Law*, cit., p. 171; *White-Collar Crime 2nd Annual*, cit., p. 499; E.A. GLYNN, *OP. CIT.*, p. 74.

⁴⁴ Così B.J. GEORGE JR., *op. cit.*, p. 390.

Altri autori hanno prescelto diversi criteri di classificazione — ad esempio A. BEQUAL, *How to Prevent Computer Crime*, cit., p. 18 — l'elencazione nel testo è, perciò, effettuata a titolo meramente indicativo.

piessità dell'ordinamento statunitense — composto, com'è noto, oltre che dalla disciplina delle *Feder Law* anche dalle molteplici manifestazioni della *State Law*⁴⁵ — che avrebbe reso frammentaria un'articolazione della materia ordinata secondo le figure di reato piuttosto che sulle fattispecie concrete. È inoltre superfluo rilevare che non si è tentato di effettuare una compiuta ricognizione dei singoli sistemi penali statali, in relazione allo specifico argomento, ma esclusivamente trarre dall'esame di certi loro aspetti alcune considerazioni. Per seguire il criterio di classificazione proposto, nel trattare della legislazione statale in materia di *computer crimes*, si è inoltre reso necessario enucleare le singole ipotesi di reato dall'insieme della disposizione incriminatrice, che nella maggior parte dei casi, è riconducibile al tipo della norma a fattispecie composita, comprendendo in un'unica disposizione distinte figure di reato⁴⁶. La particolare tecnica legislativa adottata ha anche imposto, sempre allo scopo di evitare ripetizioni superflue, di trattare in un unico contesto le questioni concernenti le soluzioni sanzionatorie adottate per le specifiche ipotesi di reato recentemente introdotte negli S.U.

II. ACCESSO ABUSIVO ED USO NON AUTORIZZATO DELL'ELABORATORE.

1. *Aspetti fenomenologici dell'accesso abusivo.*

Fra le varie e più ricorrenti ipotesi di comportamenti dannosi, o genericamente illeciti, collegati agli elaboratori, sono compresi quei casi che possono definirsi di « accesso abusivo » e di « uso non autorizzato » di un *computer* (o di un sistema di elaborazione di dati).

Per proteggere l'integrità dell'archivio informatico, o l'esclusività delle funzioni dell'elaboratore dall'inserzione di estranei, sono usualmente adottati diversi accorgimenti tecnici — come codici o parole d'ordine da digitare, chiavi, tessere magnetiche, od imprevedibili successioni di frequenze elettroniche — che consentono l'accesso all'elaboratore e possono, in relazione alle caratteristiche, selezionarne le funzioni, assicurando il compimento di una sola di esse o di un numero predeterminato (ne è un esempio la tessera del Bancomat), op-

⁴⁵ In merito alla ripartizione delle competenze fra le diverse fonti legislative, e per una compiuta elencazione delle materie affidate al potere legislativo Federale, v. M.S. BASSIOUNI, *Il diritto penale degli Stati Uniti d'America*, Milano, 1985, p. 9 ss. e L. MAYERS, *The American Legal System*, New York, 1964, p. 18.

⁴⁶ Alcune interessanti considerazioni in merito a tale tipo di fattispecie sono formula-

te da F. SGUBBI, *Uno studio sulla tutela penale del patrimonio*, Milano, 1980, p. 90 ss., ed in voce *Patrimonio (reati)*, in *Enc. dir.*, vol. XXXII, Milano, 1982, p. 331 (in part. p. 357). Esamina per altro verso questa modalità di descrizione della condotta tipica, G. VASSALLI, *Norme a fattispecie alternative e la legge Merlin*, in *Studi Antolisei*, Milano, 1965, vol. III, p. 346.

pure l'utilizzazione al pieno della funzionalità dell'elaboratore (come avviene spesso all'interno d'impresе, in cui gli utenti del sistema dispongono di strumenti di accesso diversi, che predeterminano, per quantità o qualità, le operazioni che sono chiamati a svolgere)⁴⁷. Senonché, ciascuno di questi diversi sistemi di protezione, per quanto sofisticato, può esser eluso od annullato attraverso espedienti diversi: falsificando i dispositivi di accesso (ciò che può talora integrare un autonomo reato di falso), individuando i codici segreti o superando le difese elettroniche. Inoltre, l'accesso abusivo può esser talvolta procurato attraverso il semplice ingresso nei locali in cui è situato l'elaboratore od attraverso l'allacciamento ai cavi di comunicazione quando il sistema è collegato in una rete telematica⁴⁸.

Tali condotte si sono dimostrate oltremodo pericolose, poiché spesso le limitazioni all'accesso sono il principale strumento di protezione della riservatezza dei dati memorizzati nell'archivio elettronico e dei notevoli interessi collegati alle funzioni svolte dai *computers*⁴⁹. Sino ad epoca recente negli Stati Uniti l'accesso abusivo, comunque ottenuto, è stato oggetto di studio non in quanto condotta finalizzata a se stessa, ma in quanto prodromica alla realizzazione di un altro « reato informatico » economicamente rilevante (come le frodi perpetrate attraverso l'elaboratore). Senonché le implicazioni criminologiche relative al comportamento di accesso abusivo si sono dimostrate (in coincidenza con la progressiva espansione delle grandi reti telematiche) più vaste. Si è andato, infatti, sviluppando e diffondendo un fenomeno dalle peculiari caratteristiche coincidente con l'attività dei c.d. *hackers* che, attraverso i terminali collegati alle reti telematiche, si dedicano alla metodica violazione dei sistemi di elaborazione

⁴⁷ Sulle possibilità tecniche di difesa e di superamento di sistemi informatici, cfr. D.B. PARKER, *Computer Crime*, cit., p. 276; R.D. NORMAN, *op. cit.*, p. 247 ss.; J.A. SCHWEIZER, *Computer Crime and Business Information*, New York, 1976, p. 108 ss.; M.D. SCOTT, *op. cit.*, par. 8.4; I. MURPHY, *Aspects of Hacker's Crime. High Technology, Tomfoolery or Theft?*, in *Information Data*, p. 22 (1986); J. VAN DUYN, *The Human Factor in Computer Crime*, Princeton, 1985, p. 35 ss. In Italia, cfr. G. MONALDO e G. VALLERANI, *Manuale di Informatica applicato alla revisione*, Milano, 1981, p. 184 ss.; M.G. LOSANO, *Il diritto pubblico*, cit., p. 37 ss. Alcuni casi sono riportati da R.D. NORMAN, *op. cit.*, *passim*. Sulla possibilità di stabilire frequenze alternate in modo imprevedibile per la trasmissione dei dati cfr. G. MONALDO e VALLERANI, *op. cit.*, p. 189.

⁴⁸ Cfr. L. TRIA, *op. cit.*, p. 296; A. BEQUAI, *Computer Crime*, cit., p. 41.

⁴⁹ L'interesse alla sicurezza degli impianti di elaborazione di dati si è dimostrato di tale rilievo che negli Stati Uniti è stato emesso dal Congresso Federale il « *Small Business Security and Education Computer Crime Act* » con cui vengono adottate una serie di misure a tutela delle piccole imprese e dei commercianti che intendono valersi di sistemi informatici. In particolare sono stati istituiti: un Centro di Ricerca per lo studio degli effetti dei *Computer crimes* in tali settori di attività, nonché un Centro di Informazioni capace di fornire agli imprenditori consulenze sui sistemi di sicurezza degli impianti apprestati. Al riguardo cfr. il commento alla legge di A.M. WAGNER, *op. cit.*, p. 797.

dati (*electronic trespass*)⁵⁰. Essi perseguono scopi spesso « luddistici » (come la disorganizzazione degli archivi informatici) ed allora l'accesso abusivo può associarsi alla commissione di altri *computer crimes* e, segnatamente, a manipolazioni di dati, ma talora si limitano a violare le difese del sistema. Si è, tuttavia, evidenziato come anche in quest'ultima ipotesi, in cui l'accesso abusivo non è diretto a provocare danni effettivi ed economicamente apprezzabili, esso resta una condotta intrinsecamente pericolosa per i beni connessi alla violata integrità del sistema.

Nonostante il fenomeno degli *hackers* sia di recente insorgenza, e la sua fisionomia non solo risulti imprecisa ma anche difficile da costruire per la molteplicità delle sue componenti, si è già potuto constatare che una delle sue connotazioni costanti è rappresentata dall'età adolescenziale degli autori⁵¹. Tale aspetto è stato evidenziato con la formula: « dalla criminalità dei colletti bianchi alla criminalità dei pantaloncini corti »⁵².

Negli S.U., ancor più recentemente, si è disvelato il pericoloso impiego che gli *hackers* possono fare di taluni servizi telematici posti a disposizione dei titolari di *home o personal computers*. Si tratta principalmente dei *Computer Bulletin Boards*⁵³ che offrono servizi di segreteria agli utenti consentendo la memorizzazione e la comunicazione d'informazioni, di offerte o richieste provenienti dagli utenti stessi. A seguito di alcuni episodi è risultato che gli *hackers* si valgono di tali apparati organizzativi per render pubbliche, seppur nel ristretto ambito dei destinatari del servizio, informazioni riservate sui numeri di codice, di carte di credito, sulle modalità di accesso abusivo ai sistemi informatici, o anche per proporre la vendita di materiali informatici di provenienza delittuosa⁵⁴.

⁵⁰ Sul fenomeno in generale U. SIEBER, *The International ecc.*, cit., p. 19; J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 1 ss.; A.M. WAGNER, *op. cit.*, p. 777 ss.; L. WHARTON, *op. cit.*, p. 252; J. BLOOMBECKER, *op. cit.*, p. 629 ss.; I. MURPHY, *op. cit.*, p. 22 ss.; *White-Collar Crime, Third Annual Survey of Law*, in 22 *Am. Crim. L. Rev.*, p. 494 (1984); D.B. PARKER, *Fighting*, cit., p. 130 ss. Per l'attività degli *hackers* in altre nazioni: L. MENNELLY, *op. cit.*, p. 551; C. SARZANA, *Informatica, Relazione CED*, cit., p. 14; U. SIEBER, *Definition, types and extent of criminal activity in computerized environment*, Relazione al Convegno CED, cit., p. 20. Sulle « prodezze » degli *hackers* francesi si veda *Le Matin* del 20 luglio 1986, p. 1 s. e F. FABIANI, *La beffa di Parigi, tre studenti nel cervello della difesa*, *La Repubblica* del 21 luglio 1986. La redazione del quotidiano francese ha anche organizzato un esperimento in cui cinque *hackers* (alla presenza di diversi esperti)

sono stati messi alla prova e sono riusciti in una notte a violare i sistemi informativi d'un ufficio pubblico britannico e di un'industria francese (cfr. il resoconto sulla *Repubblica* del 13 settembre 1986).

⁵¹ J. BLOOMBECKER, *op. cit.*, p. 640; J. VAN DUYN, *op. cit.*, p. 15 s.; D.B. PARKER, *op. ult. cit.*, p. 139 ss.

⁵² J. SPREUTELS, *Gli abusi collegati all'informatica nel diritto belga*, in questa *Rivista*, 1985, p. 127; B. DE SCHUTTER, *La criminalité liée à l'informatique*, in *Rev. dr. pen. crim.*, 1985, p. 388.

⁵³ Su questi fenomeni si vedano i recenti lavori di J.T. SOMA, P.J. SMITH e R.D. SPRAGUE, *op. cit.*, e di J. GILBERT, *Computer Bulletin Board Operator Liability for User Misuse*, in 54 *Fordham L. Rev.*, p. 439 (1985), nonché di I. MURPHY, *op. loc. cit.*

⁵⁴ Sulla fenomenologia degli illeciti realizzati attraverso tali sistemi cfr. J. GILBERT, *op. cit.*, *passim*.

2. (segue) ...e dell'uso non autorizzato.

Nell'esperienza statunitense la nozione di accesso abusivo si presenta parzialmente collegata a quella di uso non autorizzato dell'elaboratore. Tale correlazione è resa manifesta dall'analisi delle definizioni legislative del termine *access* in cui sono comprese oltre che attività, come il contatto o l'inserimento in un elaboratore — riconducibili all'idea di accesso — anche attività come l'archiviazione ed il reperimento di dati, in cui più propriamente consiste il vero e proprio uso dell'elaboratore⁵⁵. La commistione fra le due nozioni è tale che talora nella vasta legislazione sui *computer crimes* si può incontrare il termine « uso » definito allo stesso modo in cui usualmente lo è il termine « accesso » ed adoperato in suo luogo⁵⁶.

L'uso non autorizzato dell'elaboratore è tuttavia stato oggetto di autonomo interesse ed elaborazione, in talune sue manifestazioni denominate furto di tempo o di servizi⁵⁷. Si tratta d'ipotesi in cui l'agen-

⁵⁵ J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 10, notano come il termine *access* non sia definito nel *Counterfeit Access Device and Computer Fraud Act* del 1984, e reperiscono la relativa nozione nel progetto del Sen. Ribicoff del 1979, secondo cui significa: « avvicinarsi a comunicare con, archiviare dati in; prelevare dati da, od altrimenti far uso di ogni risorsa di un elaboratore, un sistema od una rete di elaboratori » S. 240. par. 1028.c. (1) in 2 *Computer L.J.*, 1980, p. 723. Definizioni di analogo contenuto sono state riprodotte nelle singole leggi statali ed in particolare in Ariz. Rev. Stat. Ann., par. 13-2301 E.1; Cal. Penal Code par. 502 (a) (1); Fla. Stat. Ann. par. 815.03 (10); Mich. Stat. Ann. par. 28.529 sec. 2 (1); N.C. Gen. Stat. par. 14-453 (1); R.I. Gen. Laws, par. 11-52-1 (A); Utah Code Ann. 76-6-702 (1); M. Crim. Law Code Ann. par. 27-169 (B); Minn. Stat., par. 609.861 (11); Mo. Rev. Stat., par. 1 (1); 18 Pa. Cons. Stat. par. 3933.2 (b). Interessante, inoltre, segnalare la breve definizione contenuta nella legge del New Mexico, in cui per « accesso » si intende semplicemente l'utilizzazione di ogni risorsa dell'elaboratore (N.M. Stat. Ann. par. 30-16A-2A).

⁵⁶ Cfr. sia il progetto di legge federale del sen. Nelson H.R. 1092 (per tale parte riportato da J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 9) in cui il termine « uso » significa « impartire istruzioni, archiviare dati, rilevare dati da, od altrimenti utilizzare le funzioni logiche, aritmetiche o di memoria di un elaboratore, di un sistema o rete di

elaboratori », sia la legge statale Colo. Rev. Stat., par. 18-5. 5-101 (1).

⁵⁷ I termini *theft of time* o *theft of service* sono utilizzati indifferentemente dalla dottrina statunitense, per quanto ad essi potrebbe venir ricondotto un significato parzialmente diverso. Tali denominazioni sono ormai di universale impiego; così, solo indicativamente, oltre che nelle opere americane citate alle note precedenti, v. W.H. HYMAN, *Larceny Enters the Electronic Age: The Problem of Preventing and Detecting Computer Crime*, in 18 *Gonzaga L. Rev.*, 517, part. 520 (1982/83); *White-Collar Crime: A Survey of Law*, cit., p. 371; *White-Collar Crime Second*, cit., p. 499; A. BEQUAL, *op. cit.*, p. 13; R.I. ITKIN, *Misappropriation of computer services, the need to enforce civil liability*, in 4 *Comp. L.J.*, 401 ss. (1983).

Il termine furto di tempo è stato introdotto e recepito anche in nazioni diverse dall'America: in Germania v. K. TIEDEMANN, *op. cit.*, vol. II, p. 153; U. SIEBER, *Computer Kriminalität ecc.*, cit., p. 123; in Francia: R. GASSIN, *op. cit.*, p. 35; J. PRADÉL e C. FEUILLARD, *Les infractions commises au moyen de l'ordinateur*, in *Rev. dr. pén. et crim.*, 1985, p. 307, p. 320; in Italia: C. SARZANA, *op. cit.*, p. 26; in Belgio: ERKELENS, *La Criminalité informatique en Belgique*, *Dossier: Fraud Informatique*, cit., p. 29; J.P. SPREUTELS, *Les Infractions liées à l'informatique en droit belge*, in *Rev. dr. pén. et crim.*, 1985, p. 357, part. p. 360; in Norvegia: S. SCHØLBERG, *op. cit.*, p. 25.

te sfrutta, in assenza di specifica autorizzazione⁵⁸ e a proprio esclusivo vantaggio, le funzioni dell'elaboratore; senza perciò realizzare un più grave reato, come nel caso delle frodi informatiche.

La casistica consente di suddividere tali ipotesi a seconda che l'autore persegua o meno uno scopo di lucro⁵⁹. Nel primo gruppo possono essere ricomprese le diverse ipotesi in cui i prestatori di lavoro utilizzano il *computer* loro disponibile per organizzare un'autonoma attività imprenditoriale, che resta sommersa e celata nell'attività principale dell'impresa o del proprietario del *computer*⁶⁰. Al secondo gruppo appartengono, invece, i casi di uso motivato da una finalità ludica, e dunque le ricorrenti ipotesi di dipendenti d'impresa, o studenti, che sfruttano gli elaboratori loro disponibili per realizzare le previsioni di giochi a pronostico o per svolgere videogiochi⁶¹. Il danno derivante da queste attività può anche essere ingente, almeno per quanto risulta dai cospicui risarcimenti giudizialmente richiesti⁶²: ed ancorché non siano definitivamente chiarite le diverse voci cui imputarsi il danno, si può sin d'ora puntualizzare che oltre a danni intrinseci (consumi di energia ed usura degli impianti) ne possono eventualmente derivare altri come la cancellazione fortuita di dati, ovvero l'indisponibilità parziale della memoria dell'elaboratore a causa del suo eccessivo impegno, che ledono incisivamente i diritti degli utenti autorizzati e del titolare dell'elaboratore⁶³.

3. *La qualificazione penale di tali condotte nell'ordinamento americano.*

I tentativi operati negli S.U. di qualificare la condotta di accesso abusivo alla luce delle norme vigenti hanno prodotto esiti alquanto negativi e hanno solo consentito di metter in luce l'irriducibile divario fra talune delle nuove fattispecie concrete e le figure di reato esistenti, le quali potrebbero essere applicate solo a seguito di interpretative tali da snaturarne il significato⁶⁴.

⁵⁸ La portata del termine « senza autorizzazione » inserito nella legislazione federale è dubbia: ma certamente comprende oltre che l'accesso realizzato da persone prive di ogni autorizzazione, anche quello effettuato da persone munite di un'autorizzazione limitata che ne oltrepassino i confini, come si intende dalla espressa formulazione delle diverse fattispecie del 18 USC 1030 (1)-(3), riportate alle note 84, 85, 86; sul punto cfr. J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 9 ss.

⁵⁹ Utilizza tale criterio distintivo A.M. WAGNER, *op. cit.*, p. 782 ss.

⁶⁰ Cfr. il caso trattato in U.S. v. KELLY, 507, F. Supp. 495 (E.D. Pa. 1981) in cui un impiegato aveva con il computer dell'impresa organizzato un'attività di trascrizione di brani musicali; R.D. NORMAN, *op. cit.*, p. 233, caso N. 8 1029: il dipendente d'una compagnia di assicurazioni che, con l'elaboratore

della società, teneva la contabilità per una sua impresa di *catering*.

⁶¹ Ad es. U.S. v. SAMPSON, 6 *Computer L. Serv. Rep.* (Callaghan) 879 (N.D. Cal. 1978) un bidello che con l'elaboratore della scuola tracciava le genealogie dei cavalli.

⁶² Può risultare indicativo che nel corso del processo LUND v. COMMONWEALTH, 217 Va, 688, vennero richiesti 26.384 dollari per l'uso del tempo di un elaboratore dell'università. Per considerazioni al riguardo: L. WHARTON, *op. cit.*, p. 252; L. MENNELLY, *op. cit.*, p. 566.

⁶³ R. ITKIN, *op. cit.*, p. 405; D.B. PARKER, *Computer, cit.*, p. 33.

⁶⁴ Immaginificamente definita come l'attività di *Shoehorn* (calzar le scarpe) da K. TABER, *op. cit.*, p. 737; A.M. WAGNER, *op. cit.*, p. 787; oppure di *band* (piegare) la legislazione per applicarla ai fatti, in *White-Collar Crime, Third Annual*, cit., p. 496.

In particolare l'accesso abusivo all'elaboratore è risultato una condotta così originalmente connotata da non poter essere assimilata ad alcuna delle fattispecie tipiche previste. Nel tentativo di rinvenire una norma valida a sanzionare il fatto, seppur in maniera indiretta, si è rilevato che l'ingresso fisico nei luoghi in cui il *computer* è situato può costituire il reato di *burglary* (una sorta di violazione di domicilio)⁶⁵. Tuttavia la già scarsa efficacia della norma — la quale può servire a sanzionare solo rare ipotesi di accesso abusivo — risulta ulteriormente ridotta ove si consideri che, nella maggior parte delle legislazioni statali, è richiesto, come ulteriore requisito di tipicità del fatto, che l'azione aggressiva sia posta in essere allo scopo di commettere un reato e talora in tempo di notte⁶⁶.

A conclusioni di segno parzialmente differente è invece pervenuta l'elaborazione dottrinarica ed anche giurisprudenziale in ordine a quelle fattispecie di uso non autorizzato dell'elaboratore, denominate furto di tempo o di servizi.

Nell'ambito della *Federal Law* si è ritenuto configurabile il reato di *Mail Fraud*⁶⁷ — con cui è sanzionato l'uso della posta in comunicazioni interstatali per progettare od eseguire un piano di frode — allorché autore del fatto sia un dipendente o comunque una persona legata al titolare dell'elaboratore da un rapporto fiduciario⁶⁸. Il più noto caso di applicazione della norma riguarda l'impiegato di una società che aveva utilizzato l'elaboratore per eseguire trascrizioni musicali ed aveva propagandato la sua iniziativa attraverso il servizio postale⁶⁹.

A tale risultato si è pervenuti applicando un'interpretazione della norma incriminatrice del reato di *Mail Fraud*, che riconduce nell'elastico raggio di operatività della disposizione ogni violazione di fiducia in determinati rapporti, sino a comprendervi gli atteggiamenti disinvolti assunti da una delle parti della relazione⁷⁰. Nel caso indicato

⁶⁵ U.S. DEPARTMENT OF JUSTICE, *Computer Crime*, in *Legislative Resource Manual*, Washington, 1980, p. 2; A. BEQUAI, *Computer Crime*, cit., p. 26; L.I. KRAUSS e A. MAC GAHAN, *Computer Fraud and Countermeasures*, Englewood Cliffs, New Jersey, Prentice Hall, 1979, p. 330; E.A. GLYNN, *op. cit.*, p. 89. Prevedono tale reato gli Stati della California, New Jersey, Pennsylvania, Massachusetts, Illinois, Texas, Delaware, Florida, Virginia, New York, District of Columbia.

⁶⁶ A. BEQUAI, *op. loc. cit.*, U.S., DEPARTMENT OF JUSTICE, *op. loc. cit.*, ove si rileva inoltre come tale titolo di reato sia applicabile a rari casi come l'ingresso abusivo allo scopo di danneggiare gli impianti informatici e non ad esempio al caso di ingresso abusivo per apprendere informazioni.

⁶⁷ 18 USC par. 1341: « *Whoever having devised or intended to devise any scheme or*

artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises... for the purpose of executing such scheme or artifice... places in any post office or authorized depository for mail matter, any matter or thing, whatever to be sent or delivery by the Postal service, or takes or receives therefrom, any such matter or thing, shall be... ».

⁶⁸ L. WHARTON, *op. cit.*, p. 252; *White-Collar Crime*, Second annual survey, cit., p. 501; A. BEQUAI, *Computer Crime*, cit., p. 43; A.M. WAGNER, *op. cit.*, p. 783; B.J. GEORGE, *op. cit.*, p. 392; J.T. SOMA, *op. cit.*, p. 281.

⁶⁹ U.S. v. KELLY, 507 F. Suppl 495 (E.D. Pa. 1981).

⁷⁰ J.R. COFFEE JR., *From Tort to Crime. Some Reflections on Criminalizations of Fiduciary Breaches and the Problematic Line Between Law and Ethic*, in 19 Am. Crim. L.

si è in particolare ritenuto che il dipendente avesse con il suo comportamento « frodato il datore di lavoro dei suoi onesti e leali servizi come impiegato »⁷¹. Senonché l'orientamento interpretativo invalso per il reato di *Mail Fraud*, incentrando la struttura della fattispecie incriminatrice sulla violazione delle regole comportamentali inerenti i rapporti fiduciari, impedisce di ritenere generalmente sanzionato il furto di servizi dell'elaboratore, in quanto l'uso del *computer*, oltre ad assumere secondario rilievo nell'ambito del fatto punibile, non integra addirittura l'ipotesi di reato in assenza di una relazione a carattere fiduciario fra l'agente ed il titolare dell'elaboratore, o dell'uso del servizio postale.

Si è inoltre considerato che il fatto può costituire anche il diverso reato di *embezzlement*⁷², talora ravvisato dalla giurisprudenza in fatti analoghi come l'utilizzazione d'un aereo militare a scopi privati⁷³. Tuttavia l'applicazione di tale norma resta subordinata alla non pacifica interpretazione del concetto di « cose di valore », che costituisce l'oggetto del reato: ove questo venga riferito alle sole cose tangibili, infatti, il mero furto di servizi non acquisterebbe rilevanza penale. In un caso giudiziario si è altrimenti ritenuta la sussistenza del reato, considerando che il furto di « tempo » del *computer* è inscindibile dall'identità fisica dell'elaboratore stesso, sì da poter essere assimilato al furto del medesimo⁷⁴.

A livello statale è apparsa corretta la qualificazione del fatto nell'ambito della più generale figura del *theft of services*⁷⁵, furto di servizi, quantomeno negli Stati che hanno introdotto tale previsione di reato.

Rev., p. 126 (1981), analizza acutamente, con esiti spesso critici, la recente tendenza giurisprudenziale volta a ricondurre nell'ambito del reato di *mail fraud* la responsabilità per violazione dei doveri inerenti i rapporti fiduciari, con particolare attenzione al caso giudicato in U.S. v. BRONSON, No. 81-1035 (2d Cir.) (condanna d'un legale che aveva fornito consulenze alla controparte d'un cliente dell'associazione legale cui apparteneva). Per un inquadramento della fattispecie, con riferimenti giurisprudenziali aggiornati, cfr. *White-Collar Crime, Third Annual*, cit., p. 279. La genericità della previsione, oltre ad esser richiamata nella sentenza U.S. v. KELLY, cit., p. 498 (e sottolineata in *White-Collar Crime*, cit., p. 281) è efficacemente sintetizzata nel detto « *when in doubt charge mail fraud* », riportato da J. COFFEE, *op. cit.*, p. 126.

⁷¹ U.S. v. KELLY, 507 F Supp. 499.

⁷² U.S. DEPARTMENT OF JUSTICE, *op. ult. cit.*, p. 11; A. BEQUAI, *Computer Crime*, cit., p. 40. 18 USC par. 641: « *Whoever embezzles, steals, purloins, or knowingly converts to his own use or to the use of another, or without authority, sells, conveys or disposes of any record, voucher, money or thing of*

value of the United States ». Per *conversion* s'intende l'esercizio dei diritti del proprietario sulla cosa (BLACK'S LAW DICTIONARY, St. Paul Minn., 1979, p. 300).

⁷³ U.S. v. MAY, 625 F2d 186 (1980) (con indicazione di altri precedenti); l'imputato venne condannato per *conversion* di cose di valore, in esse ritenendosi compreso il costo del servizio e non solo la benzina consumata. Nonostante nella motivazione della sentenza si faccia in tal modo riferimento a beni immateriali, invero l'attività lesiva risulta puntualizzata su una cosa tangibile (l'aereo).

⁷⁴ U.S. v. SAMPSON, cit., p. 880: La sentenza è commentata da M.D. SCOTT, *op. cit.*, par. 8.4; J.T. SOMA, *op. cit.*, p. 283; L. WHARTON, *op. cit.*, p. 252 ed in *White-Collar Crime, Third*, cit., p. 503.

⁷⁵ La più comune definizione del *theft of service* è contenuto nel *Model penal code*, par. 223. 7: chiunque « *obtains services, which are available only for compensation, by deception or threat, or by false token or other means to avoid payment for the service* ». Le pene edittali sono proporzionate al valore dei servizi ottenuti e si dipartono da un minimo di 30 giorni di pena detentiva; cfr. U.S. DEPARTMENT OF JUSTICE, *op. cit.*, p. 6;

Alla punibilità a tale titolo dell'uso non autorizzato si frappongono, tuttavia, alcuni ostacoli derivanti dalla limitata portata operativa delle singole norme incriminatrici: talune disposizioni concernono, infatti, esclusivamente i servizi offerti al pubblico dietro compenso⁷⁶, talaltre circoscrivono l'efficacia a determinati settori di attività (usualmente quello commerciale od industriale)⁷⁷ nel cui ambito non si esauriscono le possibilità d'impiego dei sistemi di elaborazione di dati. Esplicativo al riguardo è un noto caso giudiziale concernente un dipendente del *N.Y. Board of Education*, il quale aveva utilizzato l'elaboratore dell'ente educativo per scopi personali⁷⁸: il giudizio, iniziato, non poté essere proseguito poiché, nel codice dello Stato di *New York*, il reato di *theft of services* è previsto esclusivamente in relazione ad apparecchiature utilizzate in attività commerciali od imprenditoriali, e non invece nell'istruzione⁷⁹.

Se l'inquadramento dell'uso non autorizzato di elaboratore nella figura del *theft of services* appare coerente rispetto al sistema americano che prevede tale fattispecie, tuttavia il ristretto ambito di operatività delle singole norme incriminatrici ha impedito che attraverso di esse potesse ritenersi generalmente sanzionata tale condotta.

Né per ovviare all'inesistenza od all'inapplicabilità della previsione del *theft of services* è apparso utile il ricorso alla norma incriminatrice del furto comune previsto in tutte le legislazioni statali⁸⁰. È sorta in tal caso la difficoltà di ricondurre i servizi (od il tempo) del *computer* nell'ambito del concetto di *property*, che nella maggioranza delle fattispecie incriminatrici indica l'oggetto materiale del reato, tradizionalmente costruito intorno ai beni materiali⁸¹. Si è perciò, in molte situazioni, riconosciuto che tale norma, in assenza di una modifica legislativa volta a ricomprendere nell'area della sua tutela anche i servizi dell'elaboratore, non sarebbe applicabile all'ipotesi che interessa⁸².

L.I. KRAUS e A. MACGAHAN, *op. cit.*, p. 330. Il MODEL PENAL CODE è un progetto per l'unificazione della legislazione penale americana, parzialmente adottato da alcuni Stati, cfr. in proposito M.S. BASSIUNI, *op. cit.*, p. 28.

⁷⁶ Rappresenta la limitazione derivante all'applicabilità delle norme (fra cui quella prevista nel M.P.C.) dal fatto che spesso i servizi del *computer* vengono sfruttati all'interno dell'ente o dell'impresa titolare, J. BLOOMBECKER, *op. cit.*, p. 646.

⁷⁷ Cfr. A.M. WAGNER, *op. cit.*, p. 702 e 804; R.L. ITKIN, *op. cit.*, p. 404; L. WHARTON, *op. cit.*, p. 251; G. THACKERAY, *op. cit.*, p. 308.

⁷⁸ Si tratta del caso *PEOPLE v. WEG*, 450 N.Y.S. 2d 957, ampiamente commentato dagli autori citati alla nota che precede.

⁷⁹ Cfr. *People v. Weg*, 958.

⁸⁰ Tale reato, descritto nella *common law*, con una formulazione poi riprodotta in diverse leggi statali, consiste nella criminale

apprensione ed asportazione della altrui proprietà senza il consenso del proprietario e con l'intenzione di privarlo definitivamente. Cfr. U.S. DEPARTMENT, *op. cit.*, p. 3; E.A. GLYNN, *op. cit.*, p. 90; M.D. SCOTT, *op. cit.*, par. 8.4.

⁸¹ Sulla nozione di *property* si veda l'approfondita analisi comparatistica, con un inquadramento anche storico della materia, condotta da A. ALESSANDRI, *op. cit.*, p. 46 ss., in merito all'identificazione fra il concetto di *property* ed i beni tangibili cfr. U.S. DEPARTMENT, *op. ult. cit.*, p. 3 (con riferimento alle informazioni) S.H. NYCUM, *op. cit.*, p. 530; A. BEQUAI, *Computer, cit.*, p. 28 s. L. WHARTON, *op. cit.*, p. 249; M.D. SCOTT, *op. cit.*, p. 8.4. In generale, inoltre, cfr. K. SCHULHOFER PAULSEN, *Criminal law and its processes*, Boston, 1983, p. 963 s.

⁸² Così S.H. NYCUM, *Legal Problems, cit.*, in *Wash. Un. L.Q.*, 1977, part. p. 530; L. WHARTON, *op. cit.*, p. 252.

4. La recente legislazione in materia.

La situazione così delineata, caratterizzata da una tutela a carattere frammentario ed accidentale e dalla scarsa rilevanza delle ipotesi che in concreto risultano punibili, ha condotto il Congresso Federale e più della metà degli Stati Americani ad emettere una specifica normativa. L'analisi dei diversi testi legislativi consente, tuttavia, di cogliere indicazioni divergenti in merito agli orientamenti di politica criminale seguiti.

L'accesso abusivo assurge, anzitutto, a centrale considerazione nelle fattispecie di reato introdotte a livello federale dal *Counterfeit Access Device and Computer Fraud Act* del 1984⁸³. Tale legge prevede tre distinte ipotesi di reato: la più grave consiste nella fattispecie di accesso abusivo qualificata dall'intento di apprendere informazioni riservate sull'applicazione dell'energia atomica, sulla difesa o la politica estera, e dall'ulteriore scopo di danneggiare gli Stati Uniti o favorire uno Stato straniero⁸⁴; le altre, nell'accesso abusivo qualificato: dall'intenzione di ottenere informazioni finanziarie⁸⁵, o dalle conseguenze ad esso obiettivamente riconducibili, come l'apprensione, distruzione o rilevazione di dati, contenuti in elaboratori operanti per il Governo⁸⁶.

Parimenti l'accesso abusivo acquista rilievo nell'ambito dell'*Electronic Fund Transfers Act*, volto a regolare i diritti e le responsabilità reciproci degli istituti di credito e degli utenti per alcuni servizi di tra-

⁸³ Per un commento alla legge federale cfr. L. MENNELLY, *op. cit.*, p. 261 ss.; *White-Collar Crime 3d Annual*, cit., p. 495; J.B. TOMPKINS e L.A. MAR, *op. cit.*, *passim*; i quali rilevano come il titolo del testo legislativo ripete quello apposto al progetto di legge originario presentato dal sen. Hughes, ove, oltre a prevedersi gli illeciti introdotti dalla legge, si proponeva l'introduzione di altre ipotesi di reato come la contraffazione dei dispositivi di accesso ai computers governativi e le frodi informatiche nel commercio interstatale, che non sono stati tradotti in disposizioni legislative; è dunque a causa del mancato coordinamento che il titolo è rimasto inalterato e non riflette l'effettivo contenuto del testo legislativo definitivamente approvato.

⁸⁴ 18 USC par. 1030 (a) (1): « *Whoever, knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unautho-*

rized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. or section 11 of the Atomic Energy Act of 1954, with the intent or reasons to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation ».

⁸⁵ 18 USC par. 1030 (a) (2): « *Whoever knowingly accesses a computer without authorization, ... thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 USC 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC 1681 et seq.)* ».

⁸⁶ 18 USC par. 1030 (a) (3): « *Whoever knowingly accesses a computer without authorization... and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation* ».

sferimento elettronico di fondi⁸⁷. Una delle norme inserite nel testo legislativo configura, infatti, il reato di uso illegale di tessere per Eft, contraffatte, alterate, false o ottenute mediante frode o furto nell'ambito del commercio interstatale od estero⁸⁸. Nel *Credit Card Fraud Act* è inoltre sanzionato l'uso a scopo fraudolento di carte di credito illegalmente ottenute (che negli Stati Uniti sono costituite spesso da dispositivi elettronici)⁸⁹.

La punibilità di tali fatti è, tuttavia, talora condizionata alla reiterazione della condotta criminosa, sì da impedire un'estesa applicazione della norma⁹⁰.

Volgendo l'attenzione alla legislazione emessa dai singoli Stati, ci si trova dinanzi ad un panorama composito. Taluni Stati, hanno, seguendo un orientamento diverso da quello del Congresso federale, elevato l'accesso abusivo (che, come si è rilevato, comprende anche talune ipotesi di uso non autorizzato) ad autonoma fattispecie di reato⁹¹ con una previsione che risulta idonea a sanzionare sia l'attività degli *hackers* (anche se si risolve nella mera elusione delle difese del sistema informatico), sia quella degli impiegati che sfruttano a proprio esclusivo beneficio le capacità dei *computers* a loro disposizione. Tuttavia si è rilevato che le norme che sanzionano il mero accesso abusivo, o l'uso illegittimo, risultano inutilmente severe allorché sono integrate da una definizione legislativa del termine *computer*, che non delimiti la categoria convenzionalmente: in quanto ciò comporta la criminalizzazione di fatti di modesto rilievo come la consultazione

⁸⁷ 15 USC par. 1601 ss. Il trasferimento elettronico di fondi è definito come « ogni trasferimento di fondi diverso dall'azione che sia iniziato attraverso un terminale, un telefono od un *computer* per autorizzare le istituzioni finanziarie ad operare un addebito od un accredito di somme ». Sull'*EFT Act* in general cfr. P. NUVOLONE, *La trasmissione elettronica di fondi e la tutela dell'utente*, in questa *Rivista*, 1985, p. 595; S. MACCARONE, *op. cit.*, p. 606; J. MILES, *Automated teller machines: theories of liability*, in *Fordham urb. L.J.*, 1986, p. 173.

⁸⁸ 15 USC par. 1693 (n) (c); al riguardo J.T. SOMA, *op. cit.*, p. 284; *White-Collar Crime, A survey*, cit., p. 361 ss.; inoltre C. SARZANA, *op. cit.*, p. 24; L. TRIA, *op. cit.*, p. 283 ss.

⁸⁹ Sull'applicabilità del *Credit Card Abuse Act*: U.S. DEPARTMENT OF JUSTICE, *op. ult. cit.*, p. 10; L.I. KRAUSS e MAC GAHAN, *op. cit.*, p. 330; G. THACKERAY, *op. cit.*, p. 300; B.J. GEORGE JR., *op. cit.*, p. 398. La legge riguarda i dispositivi di accesso compresi i numeri di conto od i codici segreti che possono esser usati per ottenere denaro. Le condotte vietate sono l'uso, il traffico ed il possesso di dispositivi di accesso contraffatti con intento fraudolento.

⁹⁰ La legge da ultimo richiamata, richiede il possesso di 15 o più dispositivi di accesso, con intento di frode o l'uso di 10 per un anno, affinché il fatto sia punibile; al riguardo cfr. G. THACKERAY, *op. cit.*, p. 300 ss.; B.J. GEORGE JR., *op. cit.*, p. 398.

⁹¹ Chiunque « accede (...) ad un *computer*, una rete di elaborazione di dati intenzionalmente e senza autorizzazione » Ariz. Crim. Cod. par. 13-2316 (B); con formulazioni anche diverse: Cal. pen. Code par. 502 (c); Colo. Rev. Stat. par. 18-5 5-102 (2); Conn. Act of May 31, 1984, n. 84-206, par. 2 (b) (1); Fla. Stat. Ann., par. 815.06 (1); Del. Code Ann. tit. 11 par. 932; Ga. Code Ann. par. 16-9-93 (b); Illinois Crim. Code sec. 16.9 (b) 1; Idaho Code, par. 18-2202 (3); Iowa Act of May 10, 1984, par. 2; N.C. Gen. Stat. par. 14-454 (b); R.I. Gen. Laws par. 11-52.3; Mich. Comp. Laws Ann. par. 752-794; Md. Crim. Law Code Ann. par. 146; Mont. Code Ann. par. 45-6-3011; N.D. Cent. Code par. 12.1-06.1-08 (2); Okla. Stat. Ann. 21.1515; 18 Pa. Cons. Stat. Ann. par. 3933; S.D. Cod. Laws Ann. par. 4313-1 (3); Tenn. Code Ann. par. 39-3-1404 (b); Utah Code Ann. par. 76-6-703; Wash. Rev. Code Ann. (per qualunque reato) 9A-5210, S.

di un'agendina informatica tascabile o l'uso d'uno forno a micro-onde⁹².

L'accesso abusivo è stato contestualmente configurato come elemento d'una fattispecie più complessa, per la cui integrazione è altresì necessario lo scopo di realizzare una frode (od anche solo di progettarla), di appropriarsi di denaro ed altre utilità⁹³, ed in talune ipotesi anche di alterare o di danneggiare i dati od i programmi⁹⁴.

Il furto di servizi dell'elaboratore è stato sanzionato autonomamente da talune leggi statali se per ottenerlo si sono dispiegati mezzi fraudolenti⁹⁵. Si è però contestata la validità del criterio così assunto per discernere fra condotte penalmente lecite ed illecite in quanto con esso si darebbe rilevanza a circostanze anche non gravi come quelle

⁹² Cfr. L. WHARTON, *op. cit.*, p. 252.

⁹³ Ariz. 13 Crim. Code par. 2316 - A chiunque « accedendo (...) senza autorizzazione ad un elaboratore, un sistema o una rete d'elaborazione di dati o parte di essi, con l'intento di progettare od eseguire uno schema od artificio per frodare, ingannare od appropriarsi di proprietà... attraverso false rappresentazioni, pretese o promesse » e con le più varie formulazioni: Cal. pen. Code, par. 502 (b); Colo. Rev. Stat. par. 18-5-5-102 (1); Fla. Stat. Ann. par. 815.06 (b); Ga Code Ann. par. 16-9-93 (a) (1); Illinois Crim. Code sec. 16-9.b (3); Idaho Code par. 18-2202 (1); Iowa Act of May 10, 1984 par. 5; Pennsylvania Rev. Stat. par. 1473.5; Mich. Comp. Laws Ann. par. 752-795; Minn. Stat. Ann. par. 609.868; Mo Ann. Stat. par. 569.096 (1) 2; Mont. Code Ann. par. 45-6-306 c 307; N.M. Stat. Ann. par. 30-16 (A) 4; N.C. Gen. Stat. par. 14-454 (a); N.D. Cent. Code par. 12.1-06.1-8 (1); Okla. Stat. Ann. 21 par. 1515; 18 Pa. Cons. Stat. Ann. par. 3933; R.I. Gen. Law par. 11-52-2, S.D. Cod. Laws Ann. par. 4313-1 (3); Tenn. Code Ann. par. 39-3-1404 (a) (1-2).

⁹⁴ Mich. Stat. Ann. 28.529 (5) « non si otterrà, intenzionalmente e senza autorizzazione, l'accesso per alterare, danneggiare o distruggere un programma per computer o i dati contenuti in esso ». È interessante segnalare la disposizione dello Stato del North Carolina che introduce una specifica ed originale figura di reato consistente nell'accesso abusivo ad un elaboratore o sistema o rete di elaborazione con l'intento di ottenere false attestazioni o qualifiche universitarie (N.C. Gen. Stat. 14-454 a. 1-2).

⁹⁵ Tale effetto consegue al combinato disposto della norma che sanziona la condotta fraudolenta volta ad ottenere servizi, e della inclusione dei servizi del computer nella più generale nozione, effettuata ai soli fini dell'applicazione delle leggi sulla criminalità in-

formatica (sicché, non è possibile ritenere i servizi tutelati dalla normativa comune). Ad esempio: « *For the purpose of title 13-2316 (...) « services » include computer time, data processing and storage functions* ». Ariz. Rev. Stat. An. par. 13-2301 (9); Cal. Pen. Code sec. 502 (a) (8); Colo Rev. Stat. 18-5-5-101 (9); Mich. Stat. Ann. par. 28.5-29 (3) (2); N.C. Gen. Stat. par. 14-453 (9); R.I. Gen. Laws par. 11-52-1 (F); Utah Crim. Code par. 76-6-702 (6); G.A. Code Ann. 16-9-92; Idaho Code par. 18-2201; Iowa Act of May 10, 1984; La Rev. Stat. Ann. par. 14-221; N.M. Stat. Ann. par 30-16 (A) 1; Okla Stat. Ann. 21 par. 1515; 18 Pa. Cons. Stat. Ann. par. 3933; S.D. Cod. Laws Ann. par. 43-4313-1 (3); Tenn. Code Ann. 39-3-1404. Ed inoltre: « *accessing, altering, damaging... any computer... with the intent to devise or executing any scheme or artifice... to control property or services by means of false or fraudulent pretenses, representations, or premises* ». Ariz. Rev. Stat. Ann. par. 13-2316A. Identiche disposizioni incriminatrici sono previste da: Cal. Pen. Code sec. 502 (b); Colo. Rev. Stat. 18-5-5-102 (1); Mich. Stat. Ann. par. 28.529 (4); N.C. Gen. Stat. par. 14-454 (a) (1) R.I. Gen. Laws par. 11-52-2; Utah Crim. Code, par. 76-6-703; Galode Ann. par. 16-9-93 (a) (1); Idaho Code, par. 18-2202 (1), Iowa, *Act of May 1984*, 10; La. Stat. Ann., par. 14-222; Mont. Code Ann. par. 45-6-311 (prevede il fatto di ottenere i soli computer services come reato, in conseguenza di accesso, alterazione o distruzione di un sistema di elaborazione dati); N.M. Stat. Ann. par. 30-16 (A) 4; Okla. Stat. Ann. 21 par. 1515; 18 Pa. Stat. Ann. par. 3933; S.D. Cod. Laws Ann. par. 3-4313-1 (3); Tenn. Code Ann. 39-3-1404 (a) (1). Prevedono come autonoma e speciale previsione di reato, il *theft of computer services*: Conn. Legis. Serv., *Act of May 31, 1984*, par. 2 (c) e Del. Code Ann. tit. 11, par. 933; Minn. Stat. Ann. par. 609.89.

che precedono l'uso dell'elaboratore e non alle conseguenze di più grave portata⁹⁶.

In tema di furto di servizi la creazione di nuove fattispecie di reato non è tuttavia l'unica strada seguita dai singoli ordinamenti statali per sanzionare tale comportamento. Il medesimo risultato è stato anche raggiunto attraverso l'introduzione di disposizioni che, qualificano i servizi ed il tempo del *computer* come *property* e consentono l'estensione ad essi della normativa posta a tutela della proprietà⁹⁷.

Con le soluzioni adottate dai singoli Stati contrasta tuttavia la scelta operata dal Congresso americano, che nel *Counterfeit Access Device and Computer Fraud Act* ha invece esplicitamente disposto che non è penalmente perseguibile il mero uso, seppur non autorizzato, degli elaboratori appartenenti agli enti pubblici o privati indicati nella legge⁹⁸. Peraltro siffatta scelta non appare secondata dai diversi progetti di legge presentati al Parlamento Federale, con cui, fra l'altro, si propone di elevare alla qualifica di reato l'accesso abusivo all'elaboratore effettuato allo scopo di ottenere servizi⁹⁹.

La rilevata divergenza negli orientamenti di politica criminale risulta persino maggiore, ove si consideri che la fattispecie di cui si richiede l'introduzione, imperniandosi sull'accesso abusivo e relegando l'uso arbitrario dell'elaboratore nell'ambito dell'elemento psicologico del reato, comporterebbe addirittura un significativo arretramento del livello della punibilità per un fatto che, come si è notato, è stato ritenuto lecito in altra legge.

Oltre che dall'analisi della normativa, alcuni dati interessanti possono essere ricavati dalla pratica applicativa ed in particolare dal crescente rigore nell'esercizio dell'azione penale per tali comportamenti — estesosi sino all'incriminazione dei gestori dei *Bullettin Board*¹⁰⁰ — e ciò non solo sotto il profilo quantitativo (numero dei reati effettivamente perseguiti) ma anche sotto quello qualitativo (uso degli strumenti di coercizione e qualità delle pene irrogate)¹⁰¹, al punto che tale severità ha determinato vivaci reazioni e la formazione d'un indirizzo di pensiero favorevole alla criminalizzazione delle sole ipotesi più

⁹⁶ R.I. ITKIN, *op. cit.*, p. 406.

⁹⁷ Così per la disposizione del Code of Virginia par. 18.2-98.1: « *computer time services, subject of larceny* »; « *computer time or services, or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny under par. 18.2-178* »; nonché dell'Ala. Code par. 13A-8-10 (b) (per cui i servizi dell'elaboratore sono inclusi nella definizione di servizi oggetto del furto) e del Kansas (Stat. Ann. par. 21-3704) su cui cfr. J.T. SOMA, P.T. SMITH, R.D. SPRAGUE, *op. cit.*, p. 585; inoltre Me. Rev. Stat. Ann. tit. 17-A par. 357; Md.

Crim. Law Code Ann. par. 340 (i). Inoltre sono stati tutelati da diversi Stati i diritti degli utenti autorizzati alla ricezione dei servizi, con la creazione di norme incriminatrici del diniego di servizi (Fla. Stat. Ann. 815.06; Mo. Ann. Stat. 569.099; Nev. Rev. Stat. par. 205.477; Wyo. Stat. par. 6-3-409).

⁹⁸ 18 USC 1030 (a); v. note 85, 86, 87. Al riguardo cfr. J.T. TOMPKINS e L.A. MAR, *op. cit.*, p. 12; L. MENNELLY, *op. cit.*, p. 562.

⁹⁹ S. 240 par. 1028 (a) (1-2) riportato in 2 *Computer L.J.*, 1980, p. 722.

¹⁰⁰ Cfr. J. GERARD, *op. cit.*, p. 439.

¹⁰¹ Cfr. A.M. WAGNER, *op. cit.*, p. 777 ss.

gravi¹⁰² selezionate sulla base dell'intento, criminoso o specificamente fraudolento, che determina la condotta¹⁰³.

È stata comunque rilevata l'assoluta impotenza delle norme penali a reprimere l'attività dei c.d. *hackers*, i quali spesso essendo minorenni, beneficiano dell'impunità loro concessa da legislazioni vigenti in tutti gli Stati americani¹⁰⁴. Tuttavia tale preoccupazione può apparire sin eccessiva considerato che l'insorgenza dell'imputabilità è fissata, negli S.U., al compimento del tredicesimo anno d'età¹⁰⁵.

5. *L'accesso abusivo in Italia: sua irrilevanza penale.*

Nelle pagine che precedono si è mostrato come negli Stati Uniti si sia venuto progressivamente enucleando, dall'insieme dei comportamenti lesivi propri della criminalità informatica, la figura dell'accesso abusivo all'elaboratore considerato a prescindere dal verificarsi di ulteriori attività aggressive integranti diverse ipotesi criminose. Tale comportamento sostanzia un atto lesivo all'integrità del sistema d'elaborazione di dati che si presenta come un interesse funzionale alla tutela di altri beni, di natura personale o patrimoniale, connessi con i processi informatici.

In questo senso l'accesso abusivo all'elaboratore si profila come una fattispecie che, sia in riferimento alla condotta come in relazione all'interesse coinvolto (entrambi strettamente collegati ai nuovi strumenti tecnologici), può essere considerata estranea all'attuale sistema penale italiano. Il rilievo circa la novità della fattispecie concreta non esime, tuttavia, dalla ricerca d'una norma incriminatrice che possa applicarsi al caso, atteso che la condotta di accesso abusivo, intimamente consistente nel superamento o nell'elusione delle difese d'un sistema informatico, può di fatto atteggiarsi secondo distinte modalità commissive. Talune di queste — ancorché i fatti di accesso abusivo risultino *de jure condito* penalmente indifferenti nel loro nucleo fondamentale — potrebbero risultare attualmente sottoposte ad

¹⁰² Si mostrano contrari alla generica criminalizzazione dell'accesso abusivo e del furto di tempo: L. WHARTON, *op. loc. cit.*; A.M. WAGNER, *op. cit.*, p. 794; R.I. ITKIN, *op. cit.*, p. 403.

¹⁰³ A.M. WAGNER, *op. loc. cit.*, ritenuta la sufficienza delle sanzioni civili, sia per l'effetto deterrente che comportano, come per la riparazione del danno subito dalla vittima, segnala l'opportunità di sottoporre a sanzione penale solo le ipotesi di uso non autorizzato sostenute dall'intento fraudolento. Mentre R.I. ITKIN, *op. loc. cit.*, ritiene opportuno penalizzare tali fatti ove siano soggettivamente orientati verso la commissione d'un qualunque reato ulteriore.

¹⁰⁴ J. BLOOMBECKER, *op. cit.*, p. 640.

¹⁰⁵ Cfr. M.C. BASSIOUNI, *op. cit.*, p. 255 ss. il quale rileva come nei codici moderni, l'imputabilità sia fissata oltre i 13 anni e solo per alcuni reati, in considerazione della loro natura (ad es. per la violenza carnale) è fissata al compimento dei 14 anni. È tuttavia interessante rilevare che taluni Stati hanno stabilito, con leggi recenti, la responsabilità dei familiari per gli atti dei minori: Mass. Gen. Laws Ann. Ch. 266 par. 30 (1984-85); Mo. Ann. Stat. par. 537.045 (1985); N.M. Stat. Ann., par. 32-1-46 (1984); Tex. Fam. Code Ann. par. 3301 (1975); Ut. Stat. Ann. 15 par. 901; Wash. Rev. Code Ann. par. 9 A5210.5, Wis. Stat. Ann. par. 94370 (2); Wyo. Stat. par. 6-3-504.

autonoma sanzione. Allo scopo, si rende opportuno prendere singolarmente in considerazione le modalità più comunemente impiegate per l'accesso abusivo, senza peraltro pretendere di esaurire in siffatta indagine, il campo delle possibilità di aggressione.

In primo luogo possono, perciò, essere esaminati i casi di superamento delle difese fisiche del sistema, fra i quali acquista prioritaria considerazione l'ipotesi dell'ingresso fisico nei locali ove l'elaboratore è situato¹⁰⁶. Per quanto tale fattispecie presenti evidenti spunti di contatto con il reato di violazione di domicilio previsto dall'art. 614 cod. pen., è tuttavia d'immediato riscontro che tale disposizione (in quanto tutela un bene¹⁰⁷, diverso da quello leso attraverso la condotta in esame) non risulta applicabile alla generalità dei casi di accesso abusivo all'elaboratore realizzato attraverso la modalità descritta. Segnatamente essa non potrebbe ritenersi punibile se posta in essere da dipendenti, da visitatori, o, comunque, da persone ammesse all'interno dei locali, anche ove l'autorizzazione all'ingresso non implichi quella all'uso dell'elaboratore.

Né codesta potrebbe risultare l'unica limitazione al generalizzato ricorso all'art. 614 cod. pen. in relazione alla fattispecie concreta *de qua*: altri ostacoli potrebbero, invero, insorgere nel tentativo di ricondurre nell'ambito della nozione dell'oggetto materiale del reato — rappresentato dall'abitazione, dai luoghi di privata dimora e dalle loro appartenenze — taluni dei locali in cui gli elaboratori possono trovarsi situati. I concetti relativi sono stati elaborati dalla dottrina e dalla giurisprudenza, le quali pur evidenziando la necessità d'una correlazione fra il luogo e l'esplicazione della vita privata, od il suo uso domestico¹⁰⁸ (con l'esito di restringere il novero dei siti qualificabili come oggetto dell'art. 614 cod. pen.) hanno tuttavia seguito una tendenza estensiva nell'interpretazione del concetto di vita privata o di uso domestico¹⁰⁹. Sicché sono stati ricondotti nella sfera di tutela

¹⁰⁶ Nell'ambito dell'attuale sistema francese si è rilevato che l'accesso abusivo all'elaboratore può esser punito, se ottenuto attraverso il fraudolento ingresso nei locali in cui è situato, a titolo dell'art. 378 code pénal (P. SARGOS e M. MASSE, *op. cit.*, p. 26). In Belgio, parimenti, si è considerato che l'accesso abusivo può essere attualmente perseguito solo applicando le norme sulla protezione dei luoghi: C. ERKELENS, *La criminalité*, cit., p. 29 e J. SPREUTELS, cit., p. 360; B. DE SCHUTTER, *Trend.*, cit., p. 9 formula la proposta di ancorare la rilevanza penale del fatto alla sussistenza degli elementi del dolo specifico e della violazione di misure di sicurezza e la sua punibilità ad un atto d'impulso processuale della parte lesa. Interessante rilevare, invece, come la 2 WiKG tedesca non ha penalizzato il mero accesso abusivo; al riguardo

cf. L. PICOTTI, *La recente normativa*, cit., p. 8.

¹⁰⁷ L'interesse tutelato dalla norma è variamente individuato: per F. ANTOLISEI, *Manuale di dir. pen.*, parte spec. I, Torino, 1981, p. 187 si identifica nella pace domestica, per F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1079 nel domicilio inteso quale proiezione spaziale della persona.

¹⁰⁸ M. SINISCALCO, *Domicilio (violazione di)*, in *Enc. dir.*, vol. XIII, Milano, 1964, p. 871; F. ANTOLISEI, *Manuale*, cit., p. 188.

¹⁰⁹ Sottolineano la tendenza ad estendere il novero dei luoghi oggetto di tutela ai sensi dell'art. 614 cod. pen.: M. SINISCALCO, *op. cit.*, p. 873; M. GARAVELLI, *Locali aperti al pubblico e violazione di domicilio*, in *Giur. it.*, 1984, II, 261.

dell'art. 614 cod. pen. gli studi professionali¹¹⁰, le banche¹¹¹ e le scuole¹¹². Nonostante il manifestarsi di tali orientamenti, restano esclusi, o comunque sono solo condizionatamente compresi, nella nozione di privata dimora gli stabilimenti industriali¹¹³, gli esercizi pubblici¹¹⁴ e gli uffici pubblici¹¹⁵, nel cui ambito sono spesso operativi sistemi di elaborazione dati.

Può dunque rilevarsi come le limitazioni di ordine soggettivo ed oggettivo che si frappongono alla penale qualificazione di taluni fatti di accesso abusivo ai sensi dell'art. 614 cod. pen., impediscono di ritenere punibili alcune evenienze che appaiono per l'aspetto che interessa, di portata pari o superiore ad altre che attraverso la medesima disposizione possono essere sanzionate.

In secondo luogo, si può esaminare l'ipotesi dell'accesso abusivo attraverso il superamento delle difese informatiche del sistema, realizzato tramite l'impiego, da parte di persone non autorizzate, di numeri di codice, parole d'ordine, o tessere, adoperati per attivare o selezionare lo svolgimento delle funzioni dell'elaboratore. La considerazione che tali strumenti occorrono ad individuare le persone legittimate all'accesso al sistema di elaborazione dati — ed addirittura sono intestate talora a persone determinate, come avviene nel caso di tessere magnetiche — parrebbe giustificare la riconduzione del loro uso arbitrario nell'ambito dei reati di falsità personale, ed in particolare dell'ipotesi di sostituzione di persona prevista dall'art. 494 cod. pen.¹¹⁶. Nell'impiego del codice o della tessera potrebbe integrarsi a

¹¹⁰ Cass., Sez. I, 15 marzo 1977, CERBONE, *Cass. pen. Mass. ann.*, 1973, p. 1060.

¹¹¹ Cfr. M. GARAVELLI, *op. cit.*, p. 462; Cass. 2 aprile 1979, PASSALACQUA, *Giust. pen.*, 1980, 178; Cass. 28 giugno 1982, in *Riv. pen.* 1983, 640 (solo per la parte delimitata dagli sportelli).

¹¹² Cass., Sez. VI, 18 gennaio 1977, DE VITIS, *Riv. pen.*, 1977, p. 633 inoltre: Cass. 3 maggio 1979, DI FAZIO, *Giust. pen.*, 1980, II, 322: sede di un partito politico; Cass. 20 marzo 1973, in *Mass. pen.*, 1974, 822: ufficio turismo.

¹¹³ La questione della riferibilità della tutela del domicilio agli stabilimenti industriali è stata a lungo controversa e dibattuta; la più recente dottrina e giurisprudenza sembra tuttavia orientata a negarla, cfr. M. SINI-SCALCO, *op. cit.*, p. 874, sostenendo che nell'area della tutela non possono comprendersi i luoghi dove una persona subisce l'influenza di estranei; inoltre v. B. FERRARO, *Ancora sull'ingresso dei sindacalisti esterni nello stabilimento industriale*, in *Giur. mer.*, 1975, II, p. 248, il quale argomenta la tesi negativa anche con riguardo all'art. 20 dello Statuto dei lavoratori. Per un inquadramento della

questione con ampi riferimenti dottrinari e giurisprudenziali cfr. M. GARAVELLI, *Delitti contro la persona, codice penale*, a cura di F. BRICOLA e V. ZAGREBELSKI, parte spec., vol. II, Torino, 1984, p. 1104 s.

¹¹⁴ Cfr. Cass. 14 maggio 1981, in *Riv. pen.*, 1982, p. 110: è domicilio solo durante l'orario di chiusura; *contra*, M. GARAVELLI, *Locali aperti al pubblico*, *cit.*, p. 462, il quale ritiene incondizionatamente configurabile il reato.

¹¹⁵ Cfr. V. MANZINI, *Trattato di dir. pen.*, vol. VIII, Torino, 1951, p. 761.

¹¹⁶ Cfr. L. PICOTTI, *La falsificazione*, *cit.*, p. 958 che esaminando l'attuale qualificazione della falsificazione dei dati informatici in genere, ed escludendone la attuale punibilità, verifica anche l'ipotesi della configurabilità dell'art. 494 cod. pen. nei casi indicati. Si avanza quest'unica ipotesi, in quanto i numeri o gli altri dati immessi per ottenere l'accesso non possono considerarsi « atti » ai sensi delle norme sulla falsità documentali. Per maggiori dettagli al riguardo cfr. *infra*. Anche quando si tratti della falsificazione di carte di credito magnetiche o dell'uso conseguente, risulta esclusa la ricorribilità del falso

seconda dei casi l'estesa nozione « dell'attribuzione di qualità personale » — nel cui novero sono da ricomprendere le qualità di debitore, creditore, proprietario, datore o prestatore di lavoro — ovvero il lato concetto di sostituzione della propria all'altrui persona¹¹⁷, ed altresì potrebbe ravvisarsi il dolo specifico, consistente nel concreto intento di procurarsi il vantaggio di accedere all'elaboratore. Senza verificare tali ipotesi, pare sufficiente avanzare una determinante obiezione all'applicabilità dell'art. 494 cod. pen. al caso in esame: per l'integrazione di tale reato, è necessario che si verifichi l'induzione in errore di *taluno*, requisito che, — come si considererà più estesamente in seguito, trattando della configurabilità del reato di truffa rispetto ad alcune ipotesi di c.d. frodi informatiche¹¹⁸ — non si ritiene possa concretizzarsi nel fornire false indicazioni ad una *macchina*, quand'anche questa operi in conseguenza¹¹⁹.

A conclusioni parimenti negative si potrebbe pervenire esaminando l'ipotesi dell'accesso abusivo attraverso le vie telematiche (che può consistere nell'uso degli strumenti d'identificazione dianzi segnalati, come nell'arbitrario inserimento nelle linee telefoniche, o in altre forme di elusione delle difese elettroniche). Merita anzitutto rilevare al riguardo che la tutela accordata dal codice penale alle comunicazioni telefoniche e telegrafiche è stata estesa dall'art. 623-bis — introdotto dalla novella del 1974¹²⁰ — anche « alle trasmissioni d'immagini, suoni ed *altri dati*, su filo »; nel cui novero pare ricomprensibile anche la tipologia tecnica adottata per le trasmissioni di dati telematici che si avvalgono delle linee telefoniche¹²¹. Se per la lungimirante previsione legislativa le norme sulla riservatezza delle comunicazioni

nummario, considerato che le fattispecie incriminatrici (per il combinato disposto dagli artt. 453 ss. e 458 cod. pen.) concernono esclusivamente le carte del credito pubblico al portatore (qualità questa che le rende parificabili alla moneta). Per un elenco delle medesime: A. FAIS, voce *Falsità in monete*, in *Enc. dir.*, vol. XIV, Milano, 1968, 601 (in part. p. 607).

In Francia si è ritenuta non perseguibile l'alterazione delle tessere magnetiche, a titolo di falso, quando l'alterazione abbia ad oggetto solo la pista magnetica, mancando l'elemento dei « segni visibili » richiesto per l'integrazione del reato. Nel diverso caso in cui la carta sia intieramente contraffatta, si è, invece, ritenuto configurabile il reato previsto dall'art. 144 code pén. (contraffazione di titoli emessi da imprese pubbliche o private). Sull'argomento, molto estesamente, v. W. JEANDIDIER, *Les truquages et usages frauduleux de carte magnetique*, 1986, D, doc. 3229.

¹¹⁷ Circa il significato e la portata di tali concetti cfr. V. IACOVONE, *Il delitto di sostituzione di persona*, Napoli, 1974, p. 108 ss.; A. PAGLIARO, voce *Falsità personali*, in *Enc.*

dir., vol. XVI, Milano, 1967, p. 646 ss. Sottolinea l'ampiezza della nozione di attribuzione di qualità personali, F. CARNELUTTI, in *Falso in tessere di riconoscimento*, in *Riv. dir. civ.*, 1935, p. 194, ritenendo che possa ad essa ricondursi la falsificazione della tessera d'un ente per il dopolavoro.

¹¹⁸ *Infra* IV.

¹¹⁹ In tal senso L. PICOTTI, *La falsificazione*, op. loc. cit.

¹²⁰ Sulla riforma introdotta dalla legge 1974, n. 98, in generale: V. DI CIOLO e P. DI MUCCIO, *Le intercettazioni telefoniche*, Milano, 1984.

¹²¹ Dai lavori preparatori si evince con chiarezza che il legislatore intendeva espressamente riferirsi alle trasmissioni di dati effettuate attraverso elaboratori: cfr. V. DI CIOLO e P. DI MUCCIO, *op. cit.*, p. 38. Per quanto F. ANTOLISEI, a cura di CONTI, nelle due successive edizioni, *Manuale di diritto penale*, parte spec., I, p. 189 Milano, 1977, e *id.*, ed., Milano, 1981, p. 195 esprime alcune perplessità sulla possibile esistenza di dati non assimilabili né a suoni né a immagini, ritenendo, perciò, superflua la previsione.

possono essere applicate anche ai sistemi telematici, tuttavia per la limitatezza delle ipotesi di reato previste, pare che esse possano dispiacere solo parziali effetti in relazione alla condotta di accesso abusivo all'elaboratore.

Ed invero mentre talune attività prodromiche, fra l'altro, anche all'accesso abusivo potrebbero integrare il reato previsto dall'art. 617-*bis* cod. pen. (allorché vengano apprestati dispositivi atti oltre che all'intercettazione, delle comunicazioni dianzi indicate, anche ad impartire ordini all'elaboratore) non pare trovare invece applicazione al medesimo riguardo la norma incriminatrice posta dall'art. 617 cod. pen.¹²².

La disposizione sanziona infatti le attività d'intercettazione anche delle trasmissioni di dati, purché si attuino « fra altre persone » e « non siano dirette » all'agente. Attraverso tale precisazione si è espressamente imposta la necessità che la comunicazione intercettata presenti carattere intersoggettivo¹²³ e che l'agente sia in una situazione di estraneità rispetto ad essa¹²⁴; risulta perciò intuitivamente la differenza esistente fra la condotta delineata dalla norma in esame e quella in cui si realizza l'accesso abusivo, ove 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.

Ancorché la *ratio* che presiede all'incriminazione dei fatti previsti dall'art. 617 cod. pen. possa anche esser rinvenuta nelle ipotesi di accesso abusivo cui segua l'apprensione di dati, tuttavia la tassativa previsione delle condotte tipiche impedisce di ritenere applicabile tale norma alle situazioni in esame¹²⁵. Per tali ragioni l'esame delle norme sulla riservatezza delle trasmissioni informatiche dev'esser rinviato alla parte concernente la tutela dei dati nell'ordinamento italiano. In conclusione l'attività di accesso abusivo all'elaboratore, considerata indipendentemente dal verificarsi di un'ulteriore e specifica ipotesi d'illecito, non sarebbe compresa in alcuna delle fattispecie penali poste dall'attuale ordinamento, mentre solo talune delle modalità attraverso le quali può essere realizzato risulterebbero autonomamente

¹²² C. ERKELENS, *op. cit.*, p. 29 ritiene, invece, applicabili le norme del codice belga sulla tutela delle trasmissioni anche all'accesso abusivo. U. SIEBER, *The International ecc.*, cit., p. 86 rileva come in Germania il § 201 StGB richieda l'intersoggettività della comunicazione, così escludendo la punibilità dell'accesso abusivo.

¹²³ L'importanza del requisito dell'intersoggettività della comunicazione (o trasmissione), è evidenziata da P.G. Gosso, *Intercettazioni telefoniche*, in *Enc. dir.*, vol. XXI,

Milano, 1971, p. 889 e ANTOLISEI, *op. cit.*, 1981, p. 194.

¹²⁴ Sulla non punibilità del destinatario della comunicazione S. FOIS nell'*Introduzione* al volume *Intercettazioni telefoniche e rispetto della vita privata*, a cura della Camera dei Deputati, Segretariato generale, Roma, 1973, p. 9; V. MANZINI, *Trattato*, cit., vol. VIII, Torino, 1961, p. 863.

¹²⁵ In tal senso C. SARZANA, *Note*, cit., p. 28.

punibili. Come si è potuto ricavare anche dall'esame della legislazione statunitense, l'opportunità d'introdurre una norma volta a sanzionare tale condotta, dev'esser attentamente valutata, in quanto comporta un'apprezzabile anticipazione della sfera di punibilità rispetto all'effettiva lesione dei beni di natura patrimoniale o personale attinenti i processi di elaborazione dati; purtuttavia, l'estensione del fenomeno degli *hackers* anche nel nostro Paese potrebbe consigliare la creazione d'una specifica ipotesi di reato.

6. *L'uso non autorizzato: sua qualificazione nell'ordinamento italiano.*

Complesse questioni ermeneutiche pone la verifica della rilevanza penale della fattispecie di uso non autorizzato dall'elaboratore dianzi analizzata. Si è considerato come negli S.U. le ipotesi che interessano sono state ricondotte alla nozione di furto di servizi nota a quel sistema penale. Tale ritenendosi l'intima consistenza delle fattispecie, si può immediatamente rilevare che essa non appare ricomprensibile nel novero dei delitti contro il patrimonio od in altre disposizioni previste dalla legislazione italiana. Com'è stato più volte autorevolmente evidenziato, la tutela penale del patrimonio nel nostro ordinamento resta ancorata a modelli di proprietà¹²⁶, cui rimangono estranei alcuni interessi, pur di consistente valore economico. In particolare si è rimarcata (qualificandola anche come un retaggio sorpassato) la carenza di tutela penale verso le attività produttrici di servizi¹²⁷.

L'impossibilità di arricchire ed integrare il contenuto dei reati contro il patrimonio nel rispetto di soluzioni ermeneutiche rigorose, ricomprendendovi anche beni od interessi in forza del valore economico da essi acquisito, discende dalla constatazione che le fattispecie normative applicabili, come il furto e l'appropriazione indebita, s'imperniano sul termine « cosa ». Atteso che per una pacifica e in-contrastata interpretazione, il senso di tale termine è collegato alle entità materiali nel senso comune dell'espressione¹²⁸, e dunque ai soli

¹²⁶ Cfr. F. SGUBBI voce *Patrimonio (Reati)*, cit., p. 368; A. ALESSANDRI, *op. cit.*, p. 23 ss.

¹²⁷ Stigmatizzano tale lacuna: F. SGUBBI, voce *Patrimonio*, cit., p. 370, P. NUVOLENE, *Antinomie fossili e derivazioni nel codice penale italiano*, in *Trent'anni di diritto e procedura penale*, vol. I, Padova, 1969, p. 714.

¹²⁸ Compie un'approfondita disamina della nozione giuridica di cosa, con grande attenzione al concetto accolto nel diritto penale, S. PUGLIATTI, *Cosa (Teoria generale)*, in *Enc. dir.*, vol. IX, Milano, 1962, p. 19: alcune acute considerazioni, in merito alle con-

seguenze dell'inserzione del termine in talune fattispecie di reato contro il patrimonio, sono svolte da F. SGUBBI, *op. ult. cit.*, p. 360. Per ulteriori indicazioni al riguardo si rinvia alla manualistica ed alle opere a carattere generale, fra cui V. MANZINI, *Trattato del furto*, vol. II, Torino, 1905, p. 348; G. PECORELLA, voce *Patrimonio (Delitti contro il)*, in *Noviss. dig.*, vol. XII, Torino, 1965, p. 629 (in part. p. 642); ID., voce *Furto*, in *Enc. dir.*, vol. XVII, Milano, 1969, p. 318 (specif. p. 336); V. D'AMBROSIO, *I delitti contro il patrimonio*, in *Codice penale* a cura di F. BRICOLA e V. ZAGREBELSKY, Torino, 1984, p. 1138.

beni dotati di un substrato naturalistico, appare l'irriducibilità della nozione dei servizi in tale ambito¹²⁹.

La qualificazione giuridica di tali ipotesi non risulta del resto evoluta da quando verso la fine del XIX secolo apparvero i primi distributori automatici (meccanici); fu fin da allora autorevolmente osservato che, se si otteneva senza versare il dovuto corrispettivo la consegna di cose, il fatto risultava punibile a titolo di furto, mentre se si otteneva allo stesso modo la prestazione d'un servizio (la pesatura di un oggetto o la ripulitura delle scarpe) il fatto non era punibile ad alcun titolo¹³⁰.

Né il tentativo di aggirare gli ostacoli esistenti alla concreta qualificazione penale dell'uso non autorizzato di elaboratore, ipotizzando l'integrazione dei reati di furto (o di furto d'uso) in relazione all'elaboratore, pare condurre a diverso esito¹³¹. Si potrebbe infatti contrastare l'ipotesi dianzi formulata rilevando che per l'integrazione di entrambi tali reati è necessario che intervenga la sottrazione della cosa ed il relativo impossessamento, quanto invero non pare realizzarsi nelle fattispecie in esame. Avendo infatti riguardo ai modelli comportamentali più comuni (ed anche più verosimili) si può rilevare che l'uso non autorizzato dell'elaboratore si realizza *in loco*, senza che si presentino l'opportunità o ragioni pratiche per assoggettare l'impianto od una sua derivazione a qualunque forma di dislocazione, mentre il medesimo strumento resta accessibile o disponibile al proprietario, il quale può continuare ad adoperarlo.

Nonostante le nozioni di sottrazione e d'impossessamento, nell'elaborazione dottrinarina, siano andate progressivamente svincolandosi dell'iniziale rappresentazione figurata e le relative formule descrittive — quali la *contrectatio*, l'*amotio*, l'*ablatio* e l'*illatio*¹³² — siano state abbandonate facendo luogo a formule astratte, appare tuttavia implicito corollario della fattispecie in esame che l'agente abbia acquistato

¹²⁹ Con specifico riguardo ai servizi forniti dall'elaboratore: C. SARZANA, *Note*, cit., p. 28.

¹³⁰ Sul punto v. MANZINI, *op. ult. cit.*, p. 263; ID., *Trattato di diritto penale*, vol. IX, Torino, 1952, p. 151, e estesamente ID., *Commercio automatico e diritto penale*, in *Riv. pen.*, 1905, p. 17.

¹³¹ In sostanza le conclusioni cui può giungersi non paiono dissimili da quelle accolte in altri Stati. K. TIEDEMANN, *Criminalità*, cit., p. 621, osserva come il c.d. furto di tempo non sia punibile nell'ordinamento tedesco occidentale a titolo di furto, poiché l'azione lesiva non si porta su un oggetto materiale, come richiesto dalla norma del par. 242 StGB. Egli ritiene che il fatto sia punibile in via sussidiaria a titolo di Infedeltà patrimoniale (par. 266 StGB) nel ricorso eventuale dei presupposti di tale reato. V. pure U. STIEBER, *The International ecc.*, cit., p. 81 s. In Belgio si è sostenuto che tale fattispecie non configura il reato di furto, data l'insussisten-

za dell'oggetto materiale del reato, né quello di furto d'uso dell'elaboratore, non essendo realizzata alcuna sottrazione: cfr. C. ERKELENS, *op. cit.*, p. 29; e J. SPREUTELS, *op. cit.*, p. 364. Riguardo all'ordinamento francese R. GASSIN, *op. cit.*, p. 38, ritiene difficilmente applicabile il reato di furto, nell'ipotesi della sottrazione momentanea (così anche J. PRADEL e C. FEUILLARD, *op. cit.*, p. 320). B. DE SCHUTTER, *Trend*, *op. cit.*, p. 10 ritiene opportuno il ricorso alla sanzione penale del furto di tempo, in una prospettiva *de jure condendo*, solo prevedendo, quali elementi costitutivi del reato, il dolo di danno e la violazione di misure di sicurezza.

¹³² Al riguardo, F. ANTOLISEI, *Manuale di diritto penale*, parte spec. I, Milano, 1981, p. 241; G. PECORELLA, voce *Furto*, cit., p. 356. Sull'inerenza al concetto di sottrazione recepito dalla giurisprudenza dello spostamento della cosa dal luogo in cui si trova cfr. V. D'AMBROSIO, *op. cit.*, p. 1125.

la disponibilità della cosa e di essa, invece, sia stato privato il detentore¹³³.

Appare perciò dubitabile che nella maggior parte delle ipotesi di uso non autorizzato dell'elaboratore in mancanza d'indisponibilità e d'inaccessibilità della cosa possano ravvisarsi gli estremi della sottrazione ed impossessamento, in termini definitivi, come necessario per la configurabilità del furto, o meramente temporanei, come occorre invece per l'integrazione del reato di furto d'uso.

Un'interessante questione si profila invece ove s'intenda verificare se, in conseguenza del « furto di servizi » informatici, possa configurarsi il reato previsto dall'art. 624, comma 3 cod. pen. in relazione all'energia elettrica, eventualmente consumata nel corso dell'impiego della macchina¹³⁴. Tale ipotesi non sembra discostarsi molto da quella del furto di energia conseguente all'uso non autorizzato d'un televisore o di altro utensile elettrico.

Al riguardo possono essere prospettate due soluzioni di segno contrastante; innanzitutto ritenere integrato il reato sul presupposto che al vantaggio dell'agente, che utilizza l'energia come se gli appartenesse, corrisponde il danno concreto del proprietario, il quale viene ad essere depauperato della quantità di energia corrispondente al maggior esborso da lui dovuto alla società erogatrice¹³⁵.

Si potrebbe, per contro, rimarcare l'insussistenza, nella fattispecie considerata, degli elementi della sottrazione e dell'impossessamento; in quanto il consumo dell'energia è contestuale all'uso non punibile dell'elaboratore, e da questo non è possibile scinderlo, ed in quanto l'agente senza deviare l'elettricità ed apprenderla, si limita ad utilizzarne le esplicazioni¹³⁶. Tale conclusione parrebbe condivisa, seppur

¹³³ Tale dato si coglie nelle recenti costruzioni relative ai concetti in esame: cfr. F. ANTOLISEI, *op. cit.*, loc. cit., che l'identifica nell'esercizio d'un potere autonomo sulla cosa, mediante spoglio del detentore, od in chi ritiene che nel codice del 1931 si sia abbandonato il criterio spaziale per far luogo ad uno personale, G. PECORELLA, *op. ult. cit.*, 10 loc. cit.; anche V. MANZINI, *Trattato di diritto penale*, vol. IX, cit., p. 155, con specifico riguardo all'uso arbitrario della cosa.

¹³⁴ Per quanto concerne il diritto penale tedesco K. TIEDEMANN, *op. loc. cit.*, ritiene che la sottrazione di energia contestuale all'uso dell'elaboratore non possa venir automaticamente sanzionata, in quanto essa è realizzata senza l'apprestamento d'un conduttore per deviarla, come richiesto dal par. 248 StGB. Al contrario, nell'ordinamento belga, J. SPREUTELS, *op. loc. cit.*, ritiene punibile tale attività quale furto di elettricità.

¹³⁵ Tale tesi potrebbe trovar sostegno nell'ipotesi della sottrazione di energia mediante consumo in periodi di contingentamento della medesima, allorché la somministrazione sia limitata e l'utente venga privato

della quota di energia a lui disponibile integralmente. Ritiene comunque configurabile il furto di energia concomitante all'uso dell'elaboratore, A. TRAVERSI, *op. cit.*, p. 193.

¹³⁶ In conclusione, si verrebbe a ripetere il medesimo ragionamento che si effettua per determinare la non punibilità dello sfruttamento delle energie che non possono esser separate dal corpo che le emana. Così per l'energia cinetica (di cui l'agente può avvantaggiarsi facendo ad esempio trascinare la sua bicicletta da un carro) o per la c.d. energia genetica; cfr. V. MANZINI, *Trattato del furto*, cit., p. 356; G. PECORELLA, voce *Furto*, cit., p. 338. Si veda, inoltre, con riferimento al reato di peculato A. PAGLIARO, *Principi di diritto penale*, parte spec., Milano, 1983, p. 40, il quale sostiene che, ove il possesso dell'energia dipenda dal possesso della cosa che la produce, la configurabilità del reato deve esser giudicata in rapporto alla cosa. L. SEVERINO, *Il furto d'uso e delle energie*, Milano, 1933, p. 168 ss. pare aderire a tale conclusione ritenendo configurabile il furto di elettricità solo se l'agente inserisce nell'altrui presa elettrica un utensile di sua proprietà; ed al-

in maniera implicita, da coloro che per la configurabilità del furto di elettricità richiedono l'avvenuta deviazione dell'energia medesima dall'impianto del titolare e la sua immissione *altrove*¹³⁷, il che non si realizza nei casi di mero abuso di utensile.

Spostando l'attenzione su un terreno diverso da quello dell'astratta configurabilità del reato, va sottolineato che l'abuso può non dar luogo ad un consumo elettrico maggiore di quello comunque realizzato dai sistemi costantemente attivi; d'altronde la sottrazione di energia, posto che sussista, assume un rilievo marginale nella struttura del fatto lesivo e determina un depauperamento di estrema tenuità.

Tanto considerato pare opportuno, inoltre, verificare se il « furto di servizi » possa integrare il reato di appropriazione indebita nel caso in cui ricorra in capo all'agente il presupposto possessorio dell'elaboratore. Una prioritaria limitazione all'applicazione dell'art. 646 cod. pen. ai fatti di uso non autorizzato dell'elaboratore deriva dall'orientamento interpretativo, pacificamente seguito dalla dottrina e dalla giurisprudenza, secondo cui non è punibile la c.d. appropriazione indebita d'uso, consistente nel mero uso della cosa da parte del possessore (non consentito o effettuato in forma non consentita), accompagnata dall'intenzione di restituire la cosa medesima¹³⁸.

L'assunto si fonda sul rilievo dell'incompatibilità anche logica fra l'intento di restituire la cosa, che comporta il riconoscimento di un potere *potiore* su di essa, e la condotta di appropriazione, nelle sue implicazioni oggettive e soggettive, che si manifesta secondo taluni nell'inversione del possesso in proprietà¹³⁹; secondo talaltri nel com-

trove citando il caso giudiziario di due capi-operai torinesi — che avevano realizzato un'invenzione utilizzando i macchinari dell'impresa, consumando a suo scapito l'energia necessaria per farli funzionare — i quali vennero condannati per il solo furto dei materiali, sottratti e non per il consumo d'energia (*op. cit.*, p. 189). Risultato che pare confortato anche dall'opinione di F. BRUTI LIBERATI, voce *Furti minori*, in *Enc. dir.*, vol. XVII, Milano, 1969, p. 410 (in part. p. 416) che nel diverso caso del furto d'uso d'automobile, non ritiene autonomamente punibile il consumo di carburante non reintegrato dall'agente.

¹³⁷ Così A. DE MARSICO, *Delitti contro il patrimonio*, Napoli, 1951, p. 37; G. PECORELLA, *op. loc. cit.*; V. MANZINI, *op. loc. cit.*; V. D'AMBROSIO, *op. cit.*, p. 1141, che ritiene configurabile il furto di elettricità ogniquale volta la società erogatrice riceva un compenso inferiore al dovuto. Non sembra, invece, opportuno fondare la validità di tale conclusione con riferimento alle affermazioni giurisprudenziali in tema di non punibilità del consumo di energia contestuale al c.d.

« scrocco telefonico » (cfr. Cass. I, 31 dicembre 1977, NUCCHI, in *Cass. pen. Mass. ann.*, 1979, p. 84; Cass. II, 12 dicembre 1978, TOMCZAK, *Giur. it.*, 1980, II, p. 25) in quanto esse, fondandosi sulla particolare natura del contratto di utenza telefonica (nella cui economia la somministrazione d'energia non assume autonomo rilievo) riconoscono solo la non punibilità dell'uso indebito di servizi, senza trattare indipendentemente la questione dell'elettricità.

¹³⁸ Riguardo alla non configurabilità dell'appropriazione indebita d'uso, la dottrina e la giurisprudenza sono costanti sin dai tempi di F. CARRARA, *Programma del corso di diritto criminale*, parte spec., vol. IV, Luc-ca, 1867, par. 2289 e 229, se mai le divergenze concernono l'identificazione dei limiti dell'abuso non punibile.

¹³⁹ Cfr. F. CARRARA, *op. loc. cit.*; D. ANGELOTTI, *Le appropriazioni indebite*, Milano, 1933, p. 24 e 253; P. PETROCELLI, *L'appropriazione indebita*, Napoli, 1933, p. 173, che, inoltre si fonda sul riferimento all'espressa volontà del legislatore esternata nei lavori preparatori.

portamento *uti dominus* accompagnato dall'*animus* di avere la cosa come propria¹⁴⁰.

Nonostante sia uniforme la tendenza a ritenere per tali ragioni non punibile l'appropriazione indebita d'uso, si è tuttavia avvertita la necessità (onde evitare che fatti oltremodo lesivi per il proprietario possano sfuggire alle maglie della sanzione penale) di distinguere fra semplice abuso del possesso, in cui tale ipotesi consiste, e forme di effettiva appropriazione mascherate nell'apparenza del mero uso. Si è fatto ricorso per discriminare le diverse ipotesi al criterio dell'*uso esorbitante* il quale, intaccando considerevolmente la sostanza fisica od economica della cosa (ovvero esponendo questa al pericolo di perimento) si risolverebbe in un vero e proprio atto di definitivo dominio sulla cosa¹⁴¹. Tuttavia pare che il mero uso dell'elaboratore, che quantomeno nei casi più frequenti o non abnormi non comporta alcuna apprezzabile alterazione della sua struttura, non possa esser ricondotto alla nozione di uso esorbitante cui è, secondo il citato orientamento, collegato l'insorgere della penale responsabilità.

Se per tali ragioni pare arduo ricondurre l'indebito sfruttamento dei servizi informatici alla nozione di sottrazione ovvero di appropriazione di cosa, più facilmente esso potrebbe venir assimilato al diverso concetto di distrazione della cosa mobile in cui consiste la condotta tipica del reato di peculato. A tale norma si può — è superflua precisazione — far riferimento esclusivamente ove nel concreto caso ricorrano i presupposti del reato: sia soggettivo, qualifica pubblica dell'autore del fatto, sia oggettivi: appartenenza della cosa mobile alla P.A. e sussistenza in capo all'agente del possesso per ragioni di ufficio o di servizio, necessari all'integrazione della fattispecie in esame. Può infatti agevolmente rilevarsi che, attraverso l'uso non autorizzato dell'elaboratore, nelle forme e per gli intenti privati dianzi indicati, si realizzerebbe quella deviazione della cosa (elaboratore) dalle finalità cui era destinata per assoggettarla ad un *diverso scopo*, caratterizzanti la condotta distrattiva propria del reato di peculato¹⁴².

Ciò non comporta tuttavia che il furto di servizi possa nei casi indicati esser punito a tale titolo, poiché, com'è noto, esiste in Italia un cospicuo orientamento volto a ritenere penalmente lecite quelle forme di distrazione della cosa a carattere temporaneo rappresentate

¹⁴⁰ C. PEDRAZZI, voce *Appropriazione indebita*, in *Enc. dir.*, vol. I, Milano, 1958, p. 840; G.D. PISAPIA, voce *Appropriazione indebita*, in *Noviss. Dig.*, vol. I, Torino, 1957, p. 789 (in part. p. 794).

¹⁴¹ Cfr. C. PEDRAZZI, *op. cit.*, p. 844; G.D. PISAPIA, *op. loc. cit.*; V. MANZINI, *Trattato di dir. pen.*, cit., p. 815, il quale, tuttavia, pare agganciare la punibilità a considerazioni di natura soggettiva, quali il tipo di *animus* che accompagna l'abuso, piuttosto che alle concrete conseguenze di esso.

¹⁴² Riguardo alla nozione di distrazione, ed alla sua differenziazione dal concetto di

appropriazione, cfr. P. SEVERINO, *Il criterio distintivo fra appropriazione e distrazione nel peculato*, in *Cass. pen. Mass. ann.*, 1976, la quale rinviene il *principium individuationis* nella fase successiva all'elemento della deviazione del bene dalla sua destinazione originaria, che nella distrazione si risolverebbe proprio nell'uso arbitrario della cosa. Sulla riconducibilità dei fatti di mero uso della cosa alla nozione di distrazione: A. FAIS, *Sulla nozione giuridico penale del peculato d'uso e della malversazione d'uso*, in *Arch. pen.*, 1954, II, p. 5. In ordine al superamento del pregresso orientamento che ravvisava la di-

dal mero abuso del possesso e denominate peculato d'uso¹⁴³. Com'è altrettanto noto tale postulato discende dal riferimento alla volontà del legislatore chiaramente esplicitata nella relazione per la presentazione del codice ove si manifestarono le ragioni di politica criminale che avevano condotto ad espungere dal progetto definitivo la norma incriminatrice del peculato d'uso, ritenendosi sufficienti avverso tali comportamenti le sanzioni disciplinari ad essi applicabili¹⁴⁴.

Non si può, però, omettere di osservare che tale scelta è stata effettuata in relazione ad ipotesi di abuso delle macchine da scrivere, delle vetture di ufficio, le quali per diversi aspetti presentano profili di minore gravità o pericolosità rispetto all'abuso dell'elaboratore.

Nell'intento di ricondurre nella fattispecie incriminatrice i fatti di più grave portata, si è rilevato che il « peculato d'uso » non punibile sussiste intanto in quanto non si verifichi l'annullamento della destinazione pubblica propria della cosa (perciò quando essa venga distolta dalla sua originaria funzione, momentaneamente ed occasionalmente, per esservi tosto restituita), mentre sussiste il reato di peculato quando l'abuso non sia né temporaneo né eccezionale¹⁴⁵, o secondo la tesi della più recente dottrina, quando sia concretamente lesivo dell'interesse protetto dalla norma¹⁴⁶. Alla luce di tali considerazioni può rilevarsi che la punibilità dell'uso non autorizzato a titolo di peculato, lungi dall'essere generalmente esclusa, vada ancorata alla soluzione d'una questione d'ordine probatorio, concernente l'estensione effettiva dell'abuso e le concrete conseguenze ad esso correlabili, onde apprezzare se il fatto esorbits dalla nozione del peculato d'uso non punibile. Sulla base di tale premessa si può sin d'ora osservare che, normalmente, non potranno essere ricondotti alla fattispecie tipica del peculato i casi di utilizzazione occasionale o per finalità ludiche dell'elaboratore; mentre taluni dei più gravi casi di abuso, quali l'esercizio mascherato dell'impresa privata o lo svolgimento di complesse ricerche personali attraverso l'elaboratore pubblico, potrebbero essere a tale titolo sanzionati; quantomeno ove comportino, come appare verosimile, un significativo impegno della memoria dell'elaboratore tale da precluderne l'integrale disponibilità per il perseguimento della pubblica destinazione.

strazione o l'appropriazione a seconda della natura fungibile od infungibile della cosa oggetto del reato (per cui: S. RICCIO, *I delitti contro la P.A.*, Torino, 1955, p. 183; R. PANNAIN, *I delitti contro la P.A.*, Napoli, 1966, p. 71) v. le acute osservazioni svolte da M. PETRONE, *Il peculato per distrazione*, in *L'evoluzione giurisprudenziale della Corte di Cassazione*, vol. II, Roma, 1970, p. 5, part. p. 32ss.

¹⁴³ Oltre che le opere citate alla nota precedente, v. V. SCORDAMAGLIA, voce *PECULATO*, in *Enc. dir.*, vol. XXXII, Milano, 1982, p. 554; C.F. GROSSO, *I delitti contro la P.A.*,

in *Codice penale*, cit., parte spec., vol. I, p. 195; A. PAGLIARO, *op. ult. cit.*, p. 29 e la manualistica in argomento.

¹⁴⁴ *Relazione Ministeriale sul progetto del codice penale*, vol. II, p. 127.

¹⁴⁵ S. RICCIO, voce *Peculato e malversazione*, Noviss. Dig., vol. XII, Torino, 1965, p. 737 (specif. p. 742); V. MANZINI, *Trattato di dir. pen.*, vol. VIII, Torino, 1951, p. 119; R. PANNAIN, *op. cit.*, p. 79; A. PAGLIARO, *op. ult. cit.*, p. 34.

¹⁴⁶ A. FAIS, *op. ult. cit.*, p. 11; M. PETRONE, *op. cit.*, p. 36.