RICERCHE

INFORMATICA E TUTELA PENALE DEL SEGRETO INDUSTRIALE

SOMMARIO 1. Segreto industriale e *computer*. — 2. Condotte illecite. — 3. La situazione normativa in Italia. — 4. La tutela penale del segreto industriale in Germania, Gran Bretagna e Stati Uniti. — 5. Opportunità di tutela.

1. SEGRETO INDUSTRIALE E *COMPUTER*.

La catalogazione, la conservazione e l'elaborazione di tutti i dati e delle informazioni relativi all'organizzazione ed alla produttività delle varie imprese ed aziende sono oggi normalmente realizzate per mezzo degli elaboratori elettronici, la cui utilizzazione anche in ambito industriale ha tuttavia dato luogo a vari problemi di tutela. In molte nazioni, tra cui l'Italia, la crescente applicazione degli elaboratori automatici di dati e la continua espansione delle loro capacità operative[1] non hanno infatti trovato riscontro in norme capaci di garantire la sicurezza delle trasmissioni di dati, la tutela della riservatezza e la protezione dei sistemi informatici da accessi illeciti[2].

Le società e le industrie moderne dunque, sempre più dipendenti da installazioni informatiche centralizzate e da reti telematiche di comunicazione, possono subire danni particolarmente gravi soprattutto a causa della eventuale violazione di notizie segrete affidate ad un *computer*. Anni di lavoro ed investimenti di miliardi potrebbero infatti improvvisamente vanificarsi sotto lo sguardo indiscreto di un esperto programmatore nemico[3].

Se la segretezza industriale rappresenta un valido strumento per la protezione degli interessi economici dei privati imprenditori, bisogna però sottolineare come la tutela penale ad essa apprestata dal nostro ordinamento con l'art. 623 cod. pen. non sia pienamente soddisfacente e come i problemi applicativi che l'articolo citato presenta siano accentuati in caso di repressione di reati informatici. A livello di individuazione delle notizie coperte da segreto industriale si può anzitutto notare come l'attuale disposizione penale non sia in gra-

[1] Per le informazioni relative all'evoluzione ed al funzionamento degli elaboratori v. L. DADDA, *Informatica ed elettronica dei calcolatori*, in *Enc. del Novecento*, vol. III, Roma, 1978, p. 704 ss.; E. GIANNANTONIO, *Introduzione all'Informatica giuridica*, Milano, 1984.

[2] SIEBER, *The International Handbook on Computer Crime*, New York, 1987.

[3] Si calcola che ogni anno i crimini compiuti sui sistemi informatici causano danni intorno ai 5.000 miliardi di lire in tutto il mondo, anche se spesso le vittime preferiscono tacere per non suscitare allarme o per motivi di prestigio, impedendo di fatto il miglioramento della prevenzione o repressione di tali crimini. Al riguardo v. SARZANA, *Computer Technology and Crime. National and International Aspects in the International Dimensions of Contemporary Societies in the Field of Criminality and the Responses of the Movement of Social Defence*, in *Atti* dell'XI Congresso Internazionale di Difesa Sociale, Buenos Aires, 1986, p. 53.

do di tenere conto del fatto che nuove tecniche informatiche siano adottate nel settore industriale e che numerose trasformazioni si siano verificate nei modi di produzione.

I numerosi problemi interpretativi dell'art. 623 e gli scarsi riferimenti giurisprudenziali poi stanno a testimoniare l'esistenza di gravi lacune normative, destinate chiaramente ad ampliarsi in caso di applicazione della norma al mondo dell'informatica, in cui esistono innegabili difficoltà di gestione dei *computers* e delle informazioni ad essi affidate.

L'elaboratore elettronico infatti può assumere la duplice veste di mezzo e di oggetto di violazione di segreto industriale. Esso può innanzi tutto essere utilizzato come nuovo strumento di apprensione di informazioni, consentendo di procurarsi notizie, costituenti segreto industriale, attraverso la copia o la riproduzione illecita di dati segreti contenuti nella memoria dell'elaboratore, con l'ausilio di sistemi elettronici[4].

Quanto all'ipotesi del *computer* come oggetto di violazione di segreto industriale, essa si sostanzia in due aspetti fondamentali. In primo luogo come segretezza del contenuto informativo inserito nella memoria dell'elaboratore, quando le notizie siano di tipo industriale e rilevanti per la loro originalità o riservatezza[5]. In secondo luogo come segretezza dei programmi, cioè di quelle indicazioni in un determinato codice che servono ad istruire il *computer* affinché esegua una serie di operazioni atte a risolvere un particolare problema[6].

Sono proprio questi i punti deboli delle società e delle industrie moderne, alla cui protezione e garanzia la legge penale non sembra ancora in grado di poter dare un valido contributo.

2. Condotte illecite.

Gli atti che possono essere realizzati per impossessarsi di segreti di carattere scientifico o industriale, violando la sicurezza dei sistemi informatici, presentano una certa varietà, a testimonianza della estrema vulnerabilità dei dati e dei programmi elettronici[7].

Uno dei comportamenti più frequenti è l'accesso indebito del terzo alla memoria dell'elaboratore: condotta che può essere prodromica all'apprensione e conseguente utilizzazione o rivelazione di dati o notizie di tipo industriale, destinate a rimanere segrete. Normalmente la protezione di un sistema di elaborazione di dati dall'intrusione di soggetti estranei è affidata ad una serie di accorgimenti tecnici, quali tesserini magnetici, riconoscimenti a vista e codici segreti. Com'è stato osservato il mercato dell'informatica è attualmente paragonabile ad un campo minato in cui vengono sistemati trabocchetti vari per non permettere alla concorrenza di trovare la chiave dei propri sistemi[8]. In realtà non esistono mezzi di protezione sicuri, ciascuno di quelli disponibili può essere superato; d'altra parte le aziende che immagazzinano notizie riservate in un *computer* non le tutelano adeguatamente ed usano ad esempio parole d'ordine banali o facilmente individuabili. La particolare vulnerabilità dei *computers* comunque si accentua quando il sistema è collegato ad una rete telematica attra-

[4] La violazione di un segreto industriale può infatti effettuarsi a prescindere da qualsiasi contatto fisico con le informazioni, facendole comparire su un videoterminale o ordinando la riproduzione del contenuto attraverso la stampante di un elaboratore. In merito v. G. Corrias Lucente, *Informatica e Diritto Penale: elementi per una comparazione col diritto statunitense*, in *Dir. inf.*, p. 520; Sarzana, *Note sul Diritto della Informatica*, in *Giust. pen.*, 1984, I, p. 21; Sieber, *The International...*, cit., p. 93.

[5] A questo proposito v. Alessandri, *Riflessi penalistici dell'innovazione tecnologica*, Milano, 1984, p. 186, in cui si sottolinea come la questione si sostanzi in pratica in un accesso indebito alla memoria dell'elaboratore. Vedi *infra*.

[6] Relativamente al *software* ed alla sua tutela v. Alessandri, *op. cit.*, p. 185 ss.; Galtieri, *Note sulla proteggibilità dei programmi degli elaboratori elettronici*, in *Dir. aut.*, 1971, p. 425; Luzzato-Raimondi, *Patentability of Software, particularly in the European Legislation*, in *Riv. dir. ind.*, 1981, I, p. 65; Santini, *La tutela giuridica della programmazione elettronica*, in *Giur. it.*, 1968, IV, p. 225.

[7] Vulnerabilità accentuata dalla loro concentrazione ed accessibilità attraverso mezzi elettronici (G. Corrias Lucente, *op. cit.*, p. 521) e dagli scarsi investimenti fatti per sciogliere i problemi relativi alla sicurezza. Da una ricerca realizzata dall'Arthur Young International per conto della CEE su Francia, Gran Bretagna, Olanda. RFG e Italia è risultato che solo l'11% delle società ha in bilancio la voce « sicurezza informatica ».

[8] M.G. Losano, *Diritto pubblico dell'informatica*, Torino, 1986, p. 36 ss.; Sarzana, *The International Dimensions of Contemporary...*, cit., p. 51 s.; D.B. Parker, *Crime by computer*, New York, 1976.

verso l'allacciamento a cavi di comunicazione[9]. È in questo ambito infatti che operano, in numero sempre crescente, i c.d. *hackers*[10]. Si tratta di un fenomeno che tocca per lo più i giovanissimi che sono *hackers* per divertimento e non per attingere segreti a fini di lucro personale[11], ma ciò non esclude la possibilità di atti di *piratage* elettronico aventi la configurazione di un vero e proprio spionaggio scientifico od industriale. Un caso clamoroso di penetrazione di rete informatica si è ad esempio verificato lo scorso anno alla *Nasa-Spanet*, rete informatica mondiale installata per interconnettere centinaia di centri di ricerca scientifica alla grande organizzazione spaziale americana[12].

Un'altra ipotesi di violazione di segreti industriali affidati ad un *computer* ricorre quando un lavoratore addetto ad un dato settore travalichi il proprio ambito operativo, riuscendo ad ottenere informazioni normalmente escluse dalla sua sfera di conoscenza. Frequentemente infatti all'interno delle imprese informatizzate i dipendenti dispongono di strumenti diversi di accesso al *computer*, che stabiliscono *a priori* le operazioni che essi potranno svolgere sull'elaboratore e la parte della memoria-dati che potranno consultare. Superare questi limiti predeterminati senza autorizzazione si traduce in pratica in un'altra forma di accesso abusivo, operato non da un terzo estraneo, ma da un soggetto legato da un rapporto di lavoro subordinato all'imprenditore cui interessa che determinate notizie o programmi non filtrino all'esterno.

Su un piano analogo si pone poi la condotta di chi ha conosciuto le notizie in virtù di un rapporto di lavoro con l'imprenditore di tipo non subordinato. Si pensi ad esempio al consulente od al ricercatore esterno all'azienda, ai quali sono necessariamente resi accessibili in tutto od in parte dati ed informazioni[13].

Un altro sistema per entrare in possesso di segreti inseriti in un elaboratore elettronico è poi quello di sintonizzare un'antenna capace di captare la banda di frequenza tipica dei *computers* per « penetrare » le elaborazioni della macchina. I segnali elettromagnetici emessi dal *computer* infatti non sono ostacolati dalle strutture architettoniche non appositamente schermate e si può così intercettare la copia esatta di ciò che è stato immesso nel *computer*, senza alcuna possibilità di segretezza[14].

Non bisogna trascurare infine il grave problema della copia del *software*[15], che spesso acquista considerevole valore, poiché i programmi, le istruzioni permettono di trasformare il microprocessore di un *computer* in una macchina efficiente e produttiva.

L'apprensione della copia di un programma originale causa un danno notevole all'azienda che lo ha ideato, in quanto può consentire ad un'altra di rendersi concorrenziale senza alcuno sforzo di ricerca o stanziamenti, approfittando in modo illecito del lavoro e degli investimenti altrui. A questo proposito è relativamente recente il caso dell'IBM che si è rivolta alla magistratura accusando una società romana di avere plagiato il suo *software*[16]. Solo la previsione di un'apposita normativa consentirebbe di rendere un *software* meno vulnerabile, ma la soluzione non è così

[9] TRIA, *Osservazioni in tema di reati elettronici*, in *Arch. pen.*, 1984, p. 296.

[10] Termine inglese che letteralmente significa « scassinatore » ed indica chi munito di microcomputer e di « modem », cioè di un apparecchio che converte gli impulsi digitali di un *computer* in segnali analogici che possono essere trasmessi sulle normali linee telefoniche, riesce a collegarsi con banche dati telematiche di Agenzie, Enti ed industrie. Sull'argomento v. SIEBER, *op. cit.*, p. 19; SARZANA, *ult. op. cit.*, p. 51 ss.; SARZANA, *Informatica e Diritto Penale*. Relazione al Convegno: *La criminalità informatica, prevenzione e repressione*, Roma, 1986, p. 14.

[11] Celebre il caso dell'hacker che dimostrò ad un giornalista americano come fosse facile collegarsi alla rete satellite di difesa americana e quello di tre giovani francesi che riuscirono a penetrare nel cervello elettronico dell'Ecole Politecnique: *Il Messaggero* del 9 aprile 1987.

[12] A. BASSI, *Pirati e virus contro i* computer, in *Avvenire* del 23 settembre 1988.

[13] ALESSANDRI, *Riflessi penalistici...*, cit., p. 206.

[14] In *Programmi d'oro per la banda dei bit*, in *Il Sole-24 Ore* del 14 novembre 1988.

[15] Per l'analisi delle forme di tutela di tipo civilistico cfr. MINERVA, *La illiceità penale della riproduzione di programmi altrui*, in *Dir. inf.*, 1987, p. 696; RISTUCCIA, *Discordanti indirizzi giurisprudenziali in materia di* software *e videogiochi*, *ibidem*, 1986, p. 168.

[16] M. MARINACCI, *IBM contro tutti*, *MC-microcomputer*, n. 68 novembre 1987.

semplice perché al riguardo si scontrano due categorie di interessi contrapposti. Da un lato quella dei professionisti dell'informatica che da anni lamentano la mancanza di una legislazione adeguata che, col sistema del brevetto o del *copyright*, protegga il mercato del *software*; dall'altra quella delle *hardware houses* e degli utenti del *software* che paventano gli inevitabili aumenti dei prezzi del prodotto che ciò comporterebbe.

3. La situazione normativa in Italia.

La tutela penale dei segreti industriali affidati ad un elaboratore elettronico presenta diverse difficoltà; alcune in generale derivano dalla specificità degli illeciti informatici, in cui la condotta tipica è talmente particolare, rispetto alle previsioni del Diritto Penale comune, da sfuggire in gran parte alle incriminazioni tradizionali[17]. In attesa di una normativa espressamente dedicata alla materia, non resta che guardare alle attuali previsioni della legge, anche se il sistema Penale, ispirato ai principi di stretta legalità e di tipicità della fattispecie, può presentarsi poco adatto ad adeguarsi alla mutata realtà fenomenica. Tale problema si pone ad esempio per le norme a tutela del patrimonio che, risalendo agli inizi del secolo, proteggono principalmente oggetti fisici, tangibili e visibili, mentre la criminalità informatica colpisce nuove categorie di beni e prevede nuovi metodi di commissione dei reati[18].

In Italia la tutela penale del segreto industriale è affidata all'art. 623 del Codice Penale vigente che punisce « Chiunque, venuto a cognizione per ragione del suo stato o ufficio o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto »[19]. Un soggetto ha dunque diritto a che un segreto industriale di cui è titolare non sia divulgato per non perdere un vantaggio tecnico od economico[20] ed il reato può essere commesso da chi si trovi in una particolare condizione da cui sia dipesa la conoscenza del segreto. L'attuale art. 623 cod. pen. dunque, sebbene inizi con il termine « chiunque », configura un'ipotesi di reato proprio[21] sicché il suo autore deve essere qualificato da un rapporto di fatto o giuridico con il detentore del segreto[22].

Questo tipo di incriminazione non consente dunque di colpire l'*extraneus* all'azienda: il terzo può essere punito solo quando sia il destinatario della rivelazione ed abbia partecipato attivamente alla condotta dell'intraneo, anche solo istigando o determinando la rivelazione del segreto[23]. Questo aspetto della fattispecie criminosa rappresenta uno dei motivi di scarsa applicazione dell'art. 623 cod. pen. Alla querela della persona offesa, cioè interessata alla non rivelazione del segreto, si è infatti ricorso molto raramente, in quanto gli imprenditori preferiscono affidarsi a misure sanzionatorie di tipo civilistico che consentono di ottenere prontamente la cessazione

[17] Sarzana, *Note sul Diritto dell'Informatica...*, cit., p. 21; Corrias Lucente, *op. cit.*, p. 168; Sieber, *op. cit.*, p. 93; in generale Pagano, *Informatica e Diritto*, Milano, 1986.

[18] Sieber, *op. cit.*, p. 52.

[19] Analisi generali dell'art. 623 cod. pen. si trovano in: Antolisei, *Manuale di Diritto Penale*, parte sp. I, Milano, 1985, p. 211 s.; Manzini, *Trattato di Diritto Penale*, vol. VIII, 1964; Santoro, *Manuale di Diritto Penale*, vol. V, Torino, 1968, p. 341; Petrone, *Segreti (delitti contro l'inviolabilità dei)*, in *Nov. Dig.*, 1975.

[20] Crespi, *La tutela penale del segreto*, Palermo, 1952.

[21] Mazzacuva, *La tutela penale del segreto industriale*, Milano, 1979, in cui si sottolinea come l'articolo in esame colpisca solo determinate persone, munite di una particolare qualifica che ha consentito loro di venire a cognizione di notizie destinate a rimanere segrete.

[22] La nostra dottrina appare orientata nel senso di affidare all'art. 623 prevalentemente il compito di tutelare l'imprenditore dai lavoratori infedeli, v. Lega, *Osservazioni in tema di obbligo di fedeltà*, in *Riv. dir. lav.*, 1962, II, p. 124; Crespi, *op. cit.*; Siniscalco, *Rivelazione di segreti scientifici o industriali: limiti della fattispecie consumata o tentata*, in *Dir. ec.*, 1964, p. 156. Ma numerose considerazioni conducono a ritenere punibile la condotta di chi ha conosciuto le notizie in virtù di un rapporto di tipo non subordinato, v. Cessari, *Fedeltà, lavoro, impresa*, Milano, 1969, Cap. III e Alessandri, *op. cit.*, p. 196 ss.

[23] La punibilità del destinatario della rivelazione deve dunque essere ammessa quando costui abbia agito per entrare in possesso della notizia coperta da segreto, in quanto la partecipazione del terzo alla violazione commessa dal dipendente determina un obbligo di responsabilità solidale. In questo senso Quarta, *Rivelazione di segreti d'ufficio, fattispecie plurisoggettive e punibilità del partecipe non espressamente incriminato*, in *Cass. pen.*, 1981, 1448; Petrone, *op. cit.*; Pellegrino, *Lo spionaggio commerciale come atto di concorrenza sleale*, in *Foro padovano*, 1948, p. 781, vol. I.

della condotta illecita e sembrano maggiormente efficaci nel colpire tutti i soggetti che comunque abbiano contribuito alla rivelazione od utilizzazione di un segreto industriale appartenente ad un privato[24].

Senza dubbio questo concentrarsi dell'attenzione punitiva dell'art. 623 cod. pen. sulle aggressioni operate internamente all'azienda ha precise origini storiche, visto che in passato lo spionaggio esterno era un fenomeno meno esteso. Oggi invece la configurazione della tutela del segreto industriale basata sull'autore qualificato mostra qualche inadeguatezza, dal momento che non tiene sufficientemente conto delle moderne possibilità di penetrazione nella sfera riservata altrui. Soprattutto viene ad essere limitata la tutela che tale norma può offrire ai segreti industriali in ambito informatico, dove è frequente che un terzo si impadronisca direttamente di notizie riservate senza ricorrere alla cooperazione di un soggetto intraneo.

La scarsa applicabilità dell'art. 623 deriva anche dal fatto che la generica nozione di segreto industriale assume confini notevolmente incerti quando viene inserita in schemi penalistici[25]. Per individuare il settore delle notizie coperte da segreto la norma parla di « scoperte o invenzioni scientifiche o applicazioni industriali ».

Il primo termine fa senza dubbio riferimento a quelle scoperte che non si concretano in una regola tecnica ed alle quali viene perciò negata la tutela brevettuale. La scoperta consiste nel rivelare o riconoscere qualcosa di reale che prima era ignoto: un fenomeno, una legge naturale, qualsiasi elemento che arricchisca il patrimonio della conoscenza senza interferire in alcun modo nella realtà oggettiva del mondo naturale[26].

Secondo una definizione un po' approssimativa, ma sempre efficace[27], giungere ad un'invenzione significa invece realizzare una modificazione od un'innovazione dello stato oggettivo delle cose in modo da cambiare il proprio dominio delle forze naturali[28]. Sono dunque invenzioni la creazione di una nuova macchina, di uno strumento, di un dispositivo meccanico ed anche l'individuazione di nuovi procedimenti atti ad avere un'applicazione industriale.

Si ritiene che costituisca violazione del segreto industriale non solo la rivelazione di vere e proprie invenzioni, ma anche quella relativa a notizie attinenti ad un processo inventivo parziale, ancora lontano dal raggiungimento di un risultato concreto[29], ma estendere a tal punto la portata dell'incriminazione significa forse rendere la norma troppo carente dal punto di vista della tassatività[30]. Non è incongruo invece inserire nell'ambito dell'art. 623 quelle invenzioni che non presentano ancora delle successioni fenomeniche esattamente comprese, visto che spesso ai nostri giorni si ottengono nuovi risultati senza una precisa spiegazione scientifica delle dinamiche operanti. Si pensi al caso di alcune creazioni farmaceutiche, le cui capacità curative a volte non sono completamente sperimentate.

Sia la scoperta sia l'invenzione scientifica o industriale dovrebbero poi presentare un ulteriore requisito, non scritto nella norma, ma deducibile in via interpretativa: l'industrialità, e cioè la suscettibilità di applicazione professio-

[24] In particolare l'imprenditore può fare ricorso all'azione di concorrenza sleale o a quella di risarcimento del danno, le quali però precludono la successiva presentazione della querela sulla base dell'art. 623. Sull'argomento v. BRICOLA, *Profili penali della pubblicità commerciale* - Relazione presentata al Convegno di Varenna, *Riv. it. dir. e proc. pen.*, 1965, p. 744.

[25] ALESSANDRI, *Riflessi penalistici...*, cit., p. 149.

[26] CRESPI, *La tutela...*, cit., p. 187; MANZINI, *Trattato...*, cit., p. 985; MAZZACUVA, *Alcune precisazioni in tema di oggetto materiale del reato di rivelazione di segreti scientifici ed industriali*, in *Foro it.*, 1979, II, p. 308 ss.

[27] Sottolinea la difficile distinzione tra invenzione e scoperta BAVETTA, *Invenzioni industriali*, in *Enc. dir.*, vol. XXII, 1972, p. 658. Spesso infatti una scoperta è composta di atti creativi propri dell'invenzione.

[28] In questo senso CRESPI, *op. cit.*, p. 188; ALESSANDRI, *op. cit.*, p. 160; MAZZACUVA, *La tutela penale...*, cit., p. 113.

[29] Configurerebbe il reato di violazione di segreto industriale anche la rivelazione di notizie attinenti a semplici fasi di ricerca non ancora sfociate in risultati completi ed organici, secondo CRESPI, *op. cit.*, p. 189.

[30] MAZZACUVA, *op. cit.* si dedica ad un'ampia confutazione della succitata opinione di Crespi.

nale o industriale[31]. La necessità di tale requisito viene negata da chi ritiene tutelato dall'art. 623 qualunque prodotto dell'attività inventiva e di ricerca, a prescindere dalle possibilità di utilizzazione economica che possa eventualmente avere[32]. Quest'ultima impostazione è però in pieno contrasto con la prevalente dottrina che tende a sottolineare come l'art. 623 miri sempre a garantire la posizione di vantaggio che l'imprenditore trae da scoperte ed invenzioni e quindi come tale norma sia funzionale alla protezione di un mero interesse patrimoniale dell'imprenditore.

Le notizie destinate a rimanere segrete possono riguardare infine le applicazioni industriali. Queste devono essere intese non come qualcosa di autonomo, capace di ricomprendere tutto quel che si applica all'industria[33], ma come le applicazioni industriali delle scoperte o delle invenzioni. In tal modo queste ultime sono volte a scopi pratici, sono appunto industrializzate, mediante applicazione ai metodi ed ai processi di lavorazione, alle macchine od ai prodotti industriali[34]. Si ottengono così accorgimenti ed innovazioni tali da contribuire in termini reali al miglioramento ed all'aumento della produzione[35]: ogni perfezionamento tecnico infatti, per quanto modesto, può avere riflessi sulla economicità della produzione industriale, determinando ad esempio una lavorazione più rapida e meno costosa od un minore impiego di personale lavorativo[36].

Da questo breve *excursus* risulta evidente come tentare di calare nella elencazione fornita dal Codice gli aspetti propri dello sviluppo informatico sia un'operazione non priva di ostacoli. Problemi ovviamente non si pongono per i dati, memorizzati nell'elaboratore, che vertono su scoperte o invenzioni scientifiche o applicazioni industriali, mentre assai contestato è l'inserimento tra i segreti industriali dei programmi per *computer*. Di solito si cerca di adattare al programma per l'elaboratore lo schema proprio dell'invenzione, ma non manca chi sottolinea che esso non presenta in realtà quei caratteri peculiari di una invenzione[37]. Si afferma infatti che un programma nuovo consiste in un nuovo adattamento di un sistema di impostazione del lavoro della macchina, di cui è difficile stabilire il grado di originalità e di novità, e che è alla portata di ogni buon operatore del settore. Solo nei casi in cui il programma applichi tecniche del tutto particolari sulla base di un'idea geniale del programmatore potrebbe parlarsi di « creazioni inventive » inseribili nella nozione di segreto industriale penalmente tutelato[38].

Tuttavia, se ai fini dell'art. 623 cod. pen. non è richiesto che la scoperta o l'invenzione sia coperta da brevetto[39], ci si è chiesto se essa debba presentare o meno i caratteri della novità e della ori-

[31] In pratica sarebbero garantite dalla norma *de qua* solo le scoperte o invenzioni idonee ad essere industrialmente applicate e la tutela del segreto assume dunque per l'imprenditore un carattere strumentale, finalizzato alla realizzazione di una vera e propria invenzione industriale. Cfr. ROCCA, *Rivelazione di segreti scientifici o industriali*, in *Enc. for.*, VI, p. 584 ss.; MAZZACUVA, *op. cit.*, p. 113 s. Prospettiva fatta propria anche dalla Cassazione: Cass. 7 febbraio 1973, in *Giust. pen.*, 1974, II, 268 ss. con nota adesiva di Albamonte.

[32] In questo caso l'interesse tutelato dall'art. 623 sarebbe non l'esercizio dell'attività imprenditoriale ma la libertà individuale di ricerca scientifica e quindi il diritto alla riservatezza sui risultati raggiunti. V. Cass. 3 giugno 1977, in *Foro it.*, 1979, II, p. 304ss. con nota critica di Mazzacuva; BRIGNONE, *Un tema giurisprudenziale raro: l'art. 623 cod. pen., in particolare sull'industrialità e novità dell'idea inventiva e sul fondamento del segreto*, in *Cass. pen. Mass.*, 1980, p. 100 ss.

[33] Altrimenti non è più possibile trovare alcun limite per le informazioni coperte da segreto industriale secondo ALESSANDRI, *op. cit.*, p. 155.

[34] ANTOLISEI, pt. sp. cit., p. 205; MANZINI, cit., p. 985 il quale critica la dizione distintiva della norma, affermando che le invenzioni e le scoperte scientifiche sono per se stesse suscettive di applicazione industriale o professionale.

[35] MAZZACUVA, *op. cit.*, p. 115 ss.; CRESPI, STELLA, ZUCCALÀ, *Commentario al Codice Penale*, Padova, 1986, p. 1022.

[36] SANTORO, *Notazioni sul delitto di rivelazione di segreti industriali*, in *Mass. Giur. lav.*, 1974, p. 556.

[37] In questo senso si è espressa la Convenzione del Brevetto Europeo che ha affermato una netta incompatibilità tra creazione di un nuovo programma ed invenzione. In senso contrario LUZZATO-RAIMONDI, *Patentability of software...*, cit., p. 65 ss. Al riguardo v. anche A. BIANCHI, *Programmi applicativi per elaboratori elettronici ed aspetti della disciplina del segreto*, in *Dir. aut.*, 1988, I, p. 12 s. Propendono per l'applicabilità dell'art. 623 cod. pen. al *software*, CARNEVALI, *Sulla tutela giuridica del software*, in *Quadrimestre*, 1984, p. 259; TURCO, *La tutela giuridica del software*, in *Dir. aut.*, 1984, p. 150.

[38] ALESSANDRI, *op. cit.*, p. 188, ritiene però eccessivo allargare a tutti i programmi indistintamente una protezione penale adatta soltanto per taluni di essi.

[39] In questo senso sentenza Cass. 7 febbraio 1973 ed in effetti un oggetto brevettato non sempre è segreto, anzi il deposito della domanda di brevetto è uno dei momenti finali del regime di segreto (Pret. Milano, 12 dicembre 1978, in *Riv. dir. ind.*, 1979, II, 271) il segreto che può riguardare sia invenzioni suscettibili di ottenere la tutela brevettuale (in tal caso l'imprenditore potrà scegliere tra la richiesta di brevetto ed il ricorso al segreto industriale) sia innovazioni non suscettibili di attestato di privativa. Sui rapporti tra segreto e brevetto v. CAPIZZANO, *Contratto di* know-how *ed invenzione non brevettata*, in *Riv. dir. ind.*, 1974, I; MARTORANO, *Segreto e brevetto nello sfruttamento dell'invenzione industriale*, in *Riv. dir. ind.*, 1982, I, p. 223 ss.; MAZZACUVA, *op. cit.*, p. 71 ss.

ginalità. La dottrina tradizionale risolveva affermativamente il quesito in modo molto sbrigativo, ritenendo che il legislatore avesse semplicemente dimenticato di far menzione di un requisito implicito nella natura stessa della scoperta che, se non fosse nuova, non potrebbe pretendere di rimanere segreta[40]. A tanta ovvietà viene però opposta, con ragione, maggiore cautela: si reputa sufficiente che le notizie suscettibili di tutela *ex* art. 623 non siano notorie[41] e contengano un *quid novi*. Più deciso invece l'orientamento manifestato dalla giurisprudenza che ha dapprima semplicemente escluso che novità ed originalità dell'applicazione industriale rilevino in alcun modo ai fini dell'art. 623[42] ed ha poi precisato tale principio sottolineando che l'interesse alla segretezza non deve necessariamente fondarsi sulla novità delle stesse, ma può basarsi su plausibili ed apprezzabili ragioni, diverse dal carattere di novità della scoperta o del procedimento industriale[43]. Questo indirizzo interpretativo in cui può inserirsi anche una sentenza della pretura di Monza del 1983[44], con la quale si estende la tutela *ex* art. 623 cod. pen. alle originali combinazioni di dati ed elementi già conosciuti, potrebbe forse consentire l'inserimento dei *computer programs* nella nozione di segreto industriale, sebbene in pratica difficilmente l'imprenditore potrà ricevere adeguata tutela da parte di una norma limitata come l'art. 623. Inoltre la tutela penale dei programmi per elaboratori sembra attualmente esclusa dalla stessa giurisprudenza che, a proposito della copia di un programma per elaboratore elettronico, ha espressamente negato la sanzionabilità penale[45].

Per concludere l'analisi dell'art. 623 occorre rilevare come la violazione di un segreto industriale possa consistere nella rivelazione ad un terzo o nella utilizzazione a proprio od altrui profitto[46]. La prima modalità di realizzazione della fattispecie si concreta nella trasmissione della informazione, in qualunque modo effettuata, al di fuori della cerchia dei soggetti autorizzati a conoscere. Se la rivelazione prescinde da qualsiasi ulteriore specificazione, l'utilizzazione richiede invece che l'impiego di notizie segrete sia volto a proprio od altrui profitto, espressione che ha dato luogo a varie incertezze[47].

Per quel che riguarda l'elemento soggettivo, il delitto richiede il dolo generico: dunque è necessaria e sufficiente la coscienza e volontà di rivelare od utilizzare a proprio od altrui profitto la notizia coperta da segreto[48], cosicché restano in ogni caso irrilevanti per l'art. 623 le forme colpose di violazione del segreto industriale. Di conseguenza non risponde penalmente il dipendente che per imprudenza o negligenza riveli tale segreto o consenta ad un terzo di venire a conoscenza di un segreto industriale permettendogli di introdursi nell'impresa del proprio datore di lavoro.

Da quanto esposto si può indubbiamente ricavare un'intrinseca insufficienza dell'attuale tutela penale del segreto industriale, aggravata, come si è più volte sottolineato, in caso di applicazione in campo informatico.

[40] MANZINI, *op. cit.*, VIII, p. 896; ROCCA, *op. cit.*, p. 584.

[41] CRESPI, *La tutela penale...*, cit., p. 189 s.; BRIGNONE, *op. cit.*, p. 103. La nozione di notorietà comprende le informazioni di comune dominio, quelle divulgate — cioè a conoscenza di un numero indeterminato di persone — e secondo ALESSANDRI, *op. cit.*, p. 165 anche tutte le notizie che pur non essendo ancora diffuse, sono tuttavia accessibili con opportune ricerche.

[42] Cass. 7 febbraio 1973, cit.: « ... la novità e l'originalità non sono essenziali... ».

[43] Cass. 3 giugno 1977, cit.

[44] Pret. Monza 15 ottobre 1983, in *Riv. giur. lav.*, 1984, IV, 466.

[45] Cfr. Pret. Monza 26 luglio 1985, in *Dir. inf.*, 1986, che fonda la propria decisione sull'inammissibilità in sede penale dell'interpretazione analogica che, in sede civile, permette di considerare il *software* opera dell'ingegno.

[46] Non integra ovviamente l'ipotesi di reato dell'art. 623, ma determina eventualmente una responsabilità civile, la rivelazione o l'utilizzazione a proprio profitto di notizie destinate a rimanere segrete e conosciute per ragione dell'ufficio, le quali però non si riferiscano a scoperte o invenzioni scientifiche o applicazioni industriali, in Pret. Firenze 24 ottobre 1964, in *Arch. resp. civ.*, 1965, 859.

[47] La dottrina è pervenuta a diverse interpretazioni e soprattutto è dubbio se tale profitto debba essere effettivamente conseguito.

[48] MANZINI, *op. cit.*, VIII, p. 990 ss.; MAZZACUVA, *La tutela penale...*, cit., p. 120.

Relativamente ai dati memorizzati nell'elaboratore si è detto che la protezione è limitata dal fatto che l'articolo in esame configura una fattispecie di reato proprio[49], circoscrivendo la punibilità alle sole ipotesi di coloro che abbiano appreso notizie segrete, per ragione del loro stato, ufficio, professione od arte. Ovviamente gli obblighi di non abusare della propria condizione non si limitano alla segretezza delle informazioni conosciute nell'esercizio delle proprie mansioni, ma riguardano tutto ciò di cui si sia venuti a conoscenza anche per circostanze casuali. Se così non fosse non si avrebbe responsabilità penale quando un impiegato od un operaio raccogliesse dati segreti per poi rivelarli, profittando dei rapporti di amicizia o colleganza con persone addette alla stessa azienda[50].

Deve comunque sempre trattarsi di una conoscenza da parte di un soggetto qualificato, mentre per nulla rileva l'eventuale violazione commessa da un estraneo. Se dunque potrebbe essere ad esempio punita la condotta illecita del dipendente di un'impresa che si appropri di un segreto industriale affidato ad un *computer*, altrettanto non può farsi nei confronti del terzo[51], il quale potrebbe essere perseguito a titolo di concorso personale o morale. Il fatto che l'art. 623 cod. pen. richieda poi, per l'integrazione del reato, la rivelazione delle notizie ottenute in modo abusivo, riduce ancor più le capacità di applicazione della norma in esame[52].

È inoltre opinione largamente diffusa nella dottrina che non si possa ricorrere all'art. 623 quando il reo si sia procurato le notizie segrete ponendo in essere un fatto di per sé abusivo od illecito, come nel caso del dipendente dell'azienda che forzi un cassetto o una cassaforte o si introduca arbitrariamente in un locale riservato ad un dirigente per impadronirsi ad esempio delle parole chiave che consentono l'accesso ad aree riservate di un sistema informatico. In tali casi infatti le notizie sono conseguite con una attività che travalica nettamente i limiti della conoscenza funzionale e ricadono in schemi delittuosi comuni come il danneggiamento, il furto o l'appropriazione indebita[53].

A parte queste considerazioni, ulteriori incertezze relative all'applicabilità dell'art. 623 cod. pen. in campo informatico derivano dal fatto che spesso i dati ed i programmi sono destinati ad essere ceduti, dietro compenso, da una società produttrice ad un'altra, senza che per questo cessino le esigenze di tutela e di conservazione dell'esclusività del ritrovato. Se infatti un cliente a cui è stato venduto un programma lo duplica volontariamente o involontariamente, ciò causa un danno notevole all'azienda che lo ha ideato e si pone quindi il problema della possibilità di ricorrere alla norma in esame, visto che i dati ed i programmi divulgati, seppure a seguito di una remunerazione, non sembra che possano essere qualificati come segreti.

È stato inoltre affermato che il ricorrere al segreto industriale finirebbe col risultare di ostacolo ad un libero scambio delle informazioni scientifiche e tecniche[54], determinante ai fini di un ordinato e rapido sviluppo tecnologico. È questa tuttavia un'impostazione troppo rigida che non tiene conto di come la promozione della ricerca tecnologica a livello industriale possa essere risolta con più strumenti, tra i quali non può non trovare posto anche la tutela della segretezza da parte delle norme penali[55].

Quel che necessita piuttosto è un

[49] Sull'argomento v. ALESSANDRI, *op. cit.*; MAZZACUVA, *op. cit.*

[50] CRESPI, *op. cit.*; SANTORO, *Notazioni...*, cit., commento a sentenza Cass. 7 febbraio 1973.

[51] La non punibilità del terzo che violi un segreto industriale è aggravata dalla constatazione che nel nostro ordinamento l'accesso indebito all'elaboratore, considerata indipendentemente da ulteriori illeciti, è un'ipotesi delittuosa che non trova riscontro in alcuna norma incriminatrice. Inutili i tentativi di far ricorso agli artt. 614, 494 e 617 cod. pen.: v. i rilievi di SINISCALCO, *Domicilio (violabilità di)*, in *Enc. dir.*, vol. XIII, 1964, p. 874; PICOTTI, *La falsificazione dei dati informatici*, in *Dir. inf.*, 1985, p. 958; GROSSO, *Intercettazioni telefoniche*, in *Enc. dir.*, vol. XXI, 1971, p. 889, il tutto a discapito della corretta e serena conservazione delle notizie riservate relative a segreti industriali.

[52] CORRIAS LUCENTE, *op. cit.*, p. 530.

[53] MANZINI, *Trattato dir. pen. ...*, cit.; FLORIAN, *Delitti contro la libertà individuale*, in *Trattato dir. pen. it.*, 1935, p. 466; SINISCALCO, *Rivelazione...*, cit., p. 156.

[54] È di questo avviso GALTIERI, *Note sulla proteggibilità dei programmi degli elaboratori elettronici*, in *Dir. aut.*, 1971, 425.

[55] Ancora ALESSANDRI, *Riflessi penalistici...*, cit.

intervento del legislatore che miri espressamente a garantire la segretezza dei dati e dei programmi informatici e che tenga eventualmente conto delle esperienze e delle soluzioni adottate già da altre Nazioni.

4. La tutela penale del segreto industriale in Germania, Gran Bretagna e Stati Uniti.

Un'articolata tutela penale del segreto industriale fa la sua apparizione nella Repubblica Democratica Tedesca nell'ambito della normativa contro la concorrenza sleale[56]. Essa infatti punisce chiunque riveli od usi un segreto industriale illegittimamente rivelatogli da un dipendente o di cui sia venuto a conoscenza mediante una condotta contraria alla legge od al buon costume[57]. Le principali caratteristiche della legge tedesca sono dunque il fine di concorrenza sleale che deve muovere la condotta dell'agente e l'esplicito allargamento della punibilità al terzo concorrente. Tuttavia la condotta di utilizzazione o di comunicazione del segreto posta in essere da un soggetto estraneo deve sempre dipendere da una divulgazione illecita realizzata da persone operanti all'interno dell'azienda, con conseguenti inevitabili incertezze nella perseguibilità del terzo[58].

Una recente legge del maggio 1986[59] ha però introdotto la sanzione diretta degli atti di induzione alla rivelazione, dimostrando la grande sensibilità del legislatore e della dottrina tedeschi per il delicato tema relativo al segreto. Una sezione apposita di questa stessa legge è stata poi dedicata a sanzionare la falsificazione o l'alterazione dei dati e la rivelazione di segreti industriali realizzate a mezzo di *computer-crime*[60], dando vita al documento più esauriente nell'ambito della criminalità informatica e dimostrando come anche in questo settore la tutela penalistica, eventualmente legata al segreto industriale, possa assumere un rilievo sempre maggiore.

Completamente diverso è il panorama proposto dall'ordinamento britannico, caratterizzato da una scarsa propensione all'uso dello strumento penale nel campo delle violazioni di segreto industriale. La legislazione inglese non prevede *criminal offences* rivolte alla tutela del segreto industriale[61] e quindi sono state dilatate al massimo le potenzialità applicative delle figure contenute nel *Theft Act*[62]. Oggetto di *theft* però può essere solo la *property* e per quanto questo concetto venga esteso a ricomprendere anche le *intangible things*[63] è risultato problematico riconnettervi le entità immateriali proprie del segreto industriale[64]. Nessuna perplessità nasce se l'apprensione del segreto avviene mediante la definitiva sottrazione dei documenti sui quali l'informazione segreta è trascritta, in quanto in tal caso il crimine presenta tutti i caratteri materialistici propri del *theft*. Restano escluse invece le condotte che, pur violando gli interessi del titolare del segreto, investono direttamente l'informazione senza toccare

56 *Gesetz gegen der Unlauteren Wettbewerb - UWG* del 1896, perfezionata con una successiva legge del 7 giugno 1909. Per approfondimenti Ghidini, *La concorrenza sleale dalle corporazioni al corporativismo, slealtà della concorrenza e costituzione economica*, 1970, p. 46 ss.

57 Il par. 17 incrimina chi « come impiegato, lavoratore o apprendista di un'impresa comunica ad altri a scopo di concorrenza o nell'intenzione di recare danno al titolare dell'azienda, un segreto industriale ».

58 Mazzacuva, *op. cit.*, p. 93.

59 Seconda Legge per la lotta alla Criminalità Economica - Repubblica Fed. Ted. 15 maggio 1986.

60 A questo proposito v. Sarzana, *The international dimension...*, cit., p. 57; Sarzana, *La protezione penale del* software..., cit. In particolare, è prevista la punibilità di chi, venuto a conoscenza nell'esercizio o a causa delle sue mansioni di elementi contenuti in una banca dati computerizzata, li comunichi ad altri, così come è perseguibile la rivelazione di segreti dello stesso tipo cfr. Sieber, *op. cit.*, sez. 27 e sez. 29.

61 Ritiene necessaria l'introduzione di norme penali in materia Williams, *Temporary appropriation should be Theft, Criminal Law Rev.*, 1981, p. 133.

62 Sul *Theft Act* v. Smith, *The Law of Theft*, Londra, 1979; Grew, *The Theft Acts 1968 and 1978*, Londra, 1982.

63 « *Property includes money and all other property, real or personal including things in action and other intangible property* » - *Theft Act*, 1968, par. 4.

64 Nel senso che le informazioni riservate non costituiscono *intangible property* si esprimono anche Grew e Smith, *op. cit.*

il supporto materiale. Così è stata disciplinata la punibilità di chi ottenga l'informazione attraverso un uso indebito (non autorizzato) del *computer* concentrando il disvalore del fatto nella sottrazione della corrente elettrica, necessaria per il funzionamento dell'elaboratore[65]. La segretezza dei dati diviene però in questo modo del tutto marginale, mentre sarebbe più opportuno spostare l'attenzione oltre la prospettiva materialistica, considerando una vera e propria violazione il fatto che una cosa, intatta nella sua concretezza e disponibilità, sia privata del suo valore tangibile.

Se dunque in Gran Bretagna la tutela penale del segreto industriale non risulta molto sviluppata ed a maggior ragione non può trovare applicazione in campo informatico, occorre tuttavia ricordare che di recente il Regno Unito ha adottato dei provvedimenti per estendere ai *computer programs* la protezione, inclusa quella penale, del diritto d'autore[66], seguendo l'esempio in tal senso di molte altre Nazioni[67].

Per quel che riguarda l'esperienza statunitense, il settore delle notizie protetto dal *trade secret* è molto vasto. Esso comprende tutte le conoscenze che possono essere utilizzate nella produzione[68], ma alcuni Stati giungono addirittura a considerare possibile oggetto di segretezza tutte le informazioni di carattere commerciale e finanziario[69], proteggendo in tal modo ogni aspetto dell'attività di un'impresa. Sono previsti comunque anche degli elementi volti a circoscrivere l'ambito di tutela. Innanzitutto col richiedere un necessario *value* del segreto[70], valore che presuppone una valutazione concreta e puntuale della reale importanza delle informazioni sottratte[71], ed inoltre col sottoporre a tutela solo quelle informazioni che possono essere divulgate attraverso una sottrazione materiale.

Il reato di violazione di segreto industriale, introdotto di recente in alcuni Stati, è estraneo alla Legislazione Federale, la quale incrimina solo il trasporto di *goods* che siano stati *stolen, converted or taken by fraud*[72]. Anche volendo considerare il valore del supporto del tutto secondario rispetto alle informazioni in esso incorporate, la responsabilità è tuttavia ancora legata all'avvenuto trasporto di oggetti, documenti o simili[73].

Questa disposizione, applicata in campo informatico, ha consentito di sanzionare il trasporto di copie di programmi illecitamente apprese, ma secondo alcuni non è utilizzabile nei casi di trasferimento di informazioni per via elettronica da un elaboratore centrale ad un terminale in quanto gli impulsi elettronici, per la loro intangibilità, non possono essere ricondotti nel novero degli oggetti del reato in questione[74].

Differente è invece la situazione esistente nei singoli Stati. Alcuni non dispongono di figure specifiche che garantiscano il segreto scientifico ed industriale e ricorrono alle tradizionali *theft offences* relative ai beni materiali, altri fanno uso di mezzi di tutela molto precisi, che prevedono, oltre alla sottrazione o appropriazione del documento tangibile, anche le ipotesi di rivelazione e di copiatura[75]. Se infatti la maggioranza

[65] ALESSANDRI, *op. cit.*, p. 42; WILLIAMS, *Textbook of Criminal Law*, Londra, 1978, p. 689.

[66] *Copyright Computer Software Amendment Act*, 1985.

[67] V. in Francia la legge del 3 luglio 1985; in Giappone la legge n. 64 del 1985; in America la legge n. 97-180 del 1982. Cfr. AA.VV., a cura di L. RUSSI e V. ZENO-ZENCOVICH, *I programmi per elaboratore. Tutela degli utenti e delle* Software Houses, Milano, 1988. Favorevole ad una protezione dei programmi nell'ambito del diritto d'autore il « Copyright Office » di Washington. In Italia non sono ancora stati presi analoghi provvedimenti.

[68] V. ad es. le legislazioni di New Jersey, s. 2C.20-1, f; New York, s. 155.00.6.

[69] V. Illinois Crim. Code, s. 15.1; Florida Stat. Ann. 812.081 (c); Colorado Rev. Stat. par. 18.4.408 (c).

[70] Requisito richiesto da numerose legislazioni nazionali tra cui Florida Stat. Ann. s. 812.081 (c); Texas Pen. Code s. 31.05 (a) (4).

[71] ALESSANDRI, *op. cit.*, p. 152.

[72] *National Stolen Property Act* s. 2314.

[73] Famoso il caso U.S. v. Bottone, 365 F. 2d, 389, in cui la responsabilità per la sottrazione di informazioni è tuttavia legata all'avvenuto trasporto di colture di microorganismi e di fotocopie di documenti, quindi di beni dotati di tangibilità.

[74] Ward v. Superior Court, 3 Comp. L. Law Reg., 208, 1972; v. anche nota 81.

[75] Per un'analisi approfondita v. ALESSANDRI, *Riflessi penalistici...*, cit., p. 67 ss.

degli Stati ha preferito rimanere legata agli schemi tradizionali, allargando la nozione di *property* ad una serie più o meno ampia di supporti che contengono informazioni[76] (che ancora non fanno riferimento alla criminalità informatica), legislazioni più recenti incriminano le condotte di rivelazione o comunicazione o trasmissione delle informazioni segrete[77].

In America al *trade secret* ha ultimamente fatto ricorso un numero sempre maggiore di case costruttrici di *software* per proteggere i propri prodotti[78], anche se non esistono disposizioni che considerino espressamente i programmi per elaboratore come oggetto di segreto industriale[79]. Anzi relativamente al *software* sono diversi gli elementi che possono concorrere a far venir meno la segretezza e con essa la protezione giuridica, primo fra tutti la facilità di effettuazione della cosiddetta « ingegneria a rovescio » di programmi non tutelati da brevetto o da diritto d'autore, cioè la ricostruzione delle varie sequenze logiche a partire dal risultato di cui si sia lecitamente venuti a conoscenza[80].

Alcune perplessità sono sorte poi circa la possibilità di applicare ai dati ed ai programmi inseriti in un *computer*, i quali possono essere appresi a prescindere da qualsiasi contatto fisico con le informazioni, le ipotesi di repressione di spionaggio industriale legate al *theft* con conseguente qualificazione dell'oggetto del reato come *property*.

Si è già accennato come nel caso di apprensione per via elettronica di un *computer program* dall'elaboratore centrale[81] si sia affermato che gli impulsi elettronici non possono essere riconosciuti come *articles* per mancanza di tangibilità. Poiché però il programma era stato riportato su di un supporto materiale mediante l'apparecchio stampante del terminale utilizzato, la Corte ha potuto ugualmente sancire la responsabilità del soggetto che aveva effettuato tale copia.

Al di là di questa particolare ipotesi in cui è pur sempre individuabile un elemento dotato di tangibilità, si determinerebbe però una preoccupante carenza di tutela e per questo le legislazioni di alcuni Stati sono giunti a ricomprendere nella nozione di *property* i dati ed i programmi in quanto tali, indipendentemente dalla loro insistenza su un supporto materiale ed a prescindere dal loro contenuto, valore o dalla loro segretezza[82]. Più precisa però appare l'impostazione del legislatore della Florida che ha espressamente escluso che le informazioni notorie possano essere oggetto di reato, punendo l'apprensione o la rivelazione di dati concernenti informazioni riservate o costituenti segreto industriale[83].

Su un piano completamente diverso da quello relativo alla protezione del segreto industriale si pone poi la figura dell'accesso abusivo all'elaboratore, la quale ha indotto il Congresso Federale[84] e più della metà degli Stati americani ad emettere una specifica normativa. Tale ipotesi delittuosa, che non colpisce

[76] In tal senso Illinois St. ch. 38 s. 15-1 « *...property includes real estate, money ..., electricity, gas and water ..., cultures, microorganism, specimens, records, documents, blueprint, drawings...* ». Analogamente le legislazioni di Maryland Code art. 27, s. 340 e ss.; Connecticut Gen. Stat. Ann. s. 53 a-124; North Carolina Gen. Stat. s. 14-75-1.

[77] In tal senso Texas Penal Code Ann. Tit. 7, s. 31.05 (b) « *A person commits an offence if, without the owner's effective consent, he knowingly: (1) steals a trade secret; (2) makes a copy of an article rapresenting trade secret; or (3) communicates or transmits a trade secret* ». Analogamente le legislazioni di Arkansas Stat. Ann. s. 41-2207; Colorado Rev. Stat. s. 18.4.408 ed altre.

[78] SARZANA, *La protezione penale del* software..., cit.

[79] STOUT, *La brevettabilità del* software *negli USA*, in *Dir. inf.*, 1986, p. 95.

[80] *Restatement of Torts*, par. 757 (b), 1939 « ... Alcuni fattori da considerare nel determinare se un'informazione rientri nel segreto industriale sono: 1) in che misura l'informazione è conosciuta al di fuori dell'impresa, 2) in che misura è conosciuta dai dipendenti e dagli altri soggetti facenti parte dell'impresa, 3) il tipo di misure adottate per salvaguardare la segretezza, 4) il valore dell'informazione, 5) l'ammontare di lavoro o di spesa effettuata nello sviluppo dell'informazione, 6) la facilità o la difficoltà con cui l'informazione può essere acquisita o copiata in modo esatto da altri ».

[81] Ward v. Superior Court cit.; sul problema v. EPSTAIN, *Criminal liability*, p. B5-38.

[82] V. Illinois Crim. Cod. s. 15-1 « *property includes computer program sor data* ».

[83] Tale rilievo in CORRIAS LUCENTE, *op. cit.*, p. 188.

[84] Vedi al riguardo il *Counterfeit Access Device and Computer Fraud Act* del 1984 e l'*Electronic Fund Transfert Act*. Per un'analisi più approfondita rinviamo a CORRIAS LUCENTE, *op. cit.*, p. 187 ss.

direttamente beni personali o patrimoniali, ma riguarda soltanto dei sistemi informatici ad essi connessi, se non ha trovato riscontro nel nostro ordinamento in alcuna norma incriminatrice, negli Stati Uniti è stata presa in considerazione a prescindere dal verificarsi di ulteriori attività aggressive.

L'accesso abusivo è stato infatti previsto sia come elemento di un reato per la cui integrazione è necessario anche un fine fraudolento o di lucro[85], sia come fattispecie autonoma[86] per cui è punito chiunque accede ad un *computer* indipendentemente dai motivi e quindi dal carattere riservato o meno delle notizie di cui si voglia entrare in possesso.

Per tornare più specificamente al segreto industriale, si può sottolineare come negli USA la caratteristica comune delle varie forme di tutela adottate nei singoli Stati sia la loro impronta patrimoniale e l'imputazione del reato esclusivamente a carico di persone che rivestono la qualifica di dipendente[87].

L'impressione che il quadro nel suo insieme suggerisce è che anche negli S.U., come in molte altre legislazioni, siano necessari ulteriori sforzi volti a ridurre le distanze tra i bisogni di tutela di un segreto come quello industriale, strettamente connesso alla vita economica e sociale, ed i modi di attuazione dello strumento punitivo relativo alla sua violazione.

5. Opportunità di tutela.

La segretezza industriale è senza dubbio un valido strumento per la protezione di interessi economici di primaria importanza ed è destinata ad assumere particolare rilevanza in un'era industriale e tecnologica come quella attuale, in cui la tutela penale del segreto potrebbe consentire quei rapidi interventi richiesti dai gravi danni che il diffondersi della criminalità informatica causa sia nelle varie economie nazionali, sia nell'economia internazionale[88]. Numerosi dunque risultano essere gli aspetti di attualità di una disciplina a lungo ignorata dall'elaborazione dottrinale ed a cui, almeno in Italia, è stata riservata scarsa attenzione in sede legislativa, come rare sono state le applicazioni della normativa in esame.

L'orientamento internazionale, che trae ispirazione soprattutto dall'elaborazione della dottrina tedesca[89], tende a rendere più efficace la tutela del segreto in generale[90], inasprendo il trattamento sanzionatorio ed estendendo la parte precettiva della fattispecie, anche allo scopo di combattere in misura adeguata il fenomeno crescente della violazione di segreti industriali legato all'uso degli elaboratori elettronici.

Non si può tacere comunque l'esistenza anche di un'impostazione contraria, volta a segnalare l'inopportunità del ricorso all'apparato sanzionatorio offerto dal diritto penale, sulla base della considerazione che l'imprenditore ha un limitato interesse ad iniziare un'azione penale la quale, grazie alla pubblicità del processo, potrebbe aggravare ulteriormente il pregiudizio causato dalla divulgazione[91]. Proprio in questi termini si spiegherebbe la scarsità di dati giurisprudenziali relativi a procedimenti penali per il reato di violazione di segreti industriali. Se ciò è vero in alcuni casi, non dovrebbe però portare ad un'eliminazione dell'illiceità delle condotte di rivelazione o di utilizzazione di un segreto scientifico o industriale, da reprimere in quanto atte ad aggredire gravemente gli aspetti patrimoniali e concorrenziali di un'attività imprenditoriale.

È stato da più parti sottolineato che le norme penali in materia di segreto indu-

[85] Ad esempio Arizona Crim. Cod. 13-2316 (A); Minn. Stat. Ann. par. 609.869; Cal. Pen. Code par. 502 (b).

[86] Alcuni Stati hanno configurato la punibilità di chiunque accede ad un *computer* « intenzionalmente e senza autorizzazione ». Così in Ariz. Crim. Code 13-2316 (B); Cal. Pen. Code par. 502 (c); Illinois Crim. Code s. 16.9 (b) 1 ed altri.

[87] Alessandri, *op. cit.*, p. 68 ss.

[88] Sarzana, *op. ult. cit.*

[89] La collocazione geografica della Germania Federale determina infatti particolari preoccupazioni per le attività di spionaggio: cfr. Amelunxen, *Werkschuts und Kriminalitaet*, Amburgo, 1977.

[90] In questo senso Mazzacuva, *La tutela penale...*, cit., p. 238.

[91] Mazzacuva, *op. loc. cit.*

striale necessitano, soprattutto nel nostro ordinamento, di opportune riforme che tengano conto delle trasformazioni verificatesi nei modi di produzione e della introduzione di nuove tecnologie, come quelle informatiche, anche nel settore industriale. Si ritiene che il primo passo che le varie Nazioni dovrebbero compiere in questo ambito è quello di cercare di eliminare le differenze esistenti tra le proprie legislazioni, dal momento che i problemi provocati dai reati informatici sono ormai diffusi in tutti i Paesi ad alto livello tecnologico e le condotte criminose attuate in un singolo Stato, possono abbastanza agevolmente portare le proprie conseguenze al di fuori dei confini di esso. Bisogna inoltre tener conto del fatto che in futuro la criminalità informatica sarà destinata ad aumentare per l'intensificarsi dell'utilizzazione del *computer* e quindi della dipendenza dalle sue prestazioni[92].

Non ci sono dubbi che la questione della concentrazione degli sforzi per il superamento delle difficoltà relative ad una riforma del diritto penale in questo campo sarà di notevolissima importanza per il futuro. Alcune proposte sono state formulate anche nell'ambito di organizzazioni internazionali, come dimostra l'attività del Consiglio di Europa che, dopo aver posto in particolar luce l'insufficienza degli attuali sistemi sanzionatori, ha sottolineato la rilevanza dello strumento penale e la necessità di un suo potenziamento[93] per contrastare l'enorme capacità offensiva dello spionaggio industriale specie in considerazione delle nuove tecniche di raccolta delle informazioni e di intercettazione delle comunicazioni. La previsione di norme penali adatte a reprimere anche e soprattutto il fenomeno della criminalità informatica potrebbe costituire infatti un deterrente di non trascurabile importanza e potrebbe consentire una più completa difesa degli aspetti patrimoniali e concorrenziali di un'attività imprenditoriale.

A tale proposito è forse opportuno ricordare come anche la Organization for Economic Co-operation and Development (OCSE) abbia inserito nella serie degli atti che tutti gli Stati dovrebbero impegnarsi a perseguire per combattere i *computer crimes*, le varie condotte connesse alla violazione di segreto industriale[94], sottolineando la negatività sia per le singole economie nazionali, sia per l'economia internazionale, di questa forma di illecito penale.

MARIA CRISTINA PALAIA

[92] SIEBER, *The International Handbook on Computer Crime*, New York, 1987.

[93] Per l'attività del Consiglio d'Europa v. Report del 20 gennaio 1971 e Resolution n. 571 del 1974.

[94] SIEBER, *op. loc. cit.*