GIOVANNA CORRIAS LUCENTE

PRIME CONSIDERAZIONI IN TEMA DI RESPONSABILITÀ PENALE E GESTIONE DI SISTEMI INFORMATIZZATI CON PARTICOLARE RIGUARDO AI SISTEMI ESPERTI

SOMMARIO 1. Introduzione. — 2. Sistemi tradizionali e sistemi esperti. — 3. Responsabilità penali della gestione: *a*) per illeciti di natura dolosa; *b*) per illeciti di natura colposa. — 4. Responsabilità per la gestione di banche dati. — 5. Robotica e tutela penale del lavoro. — 6. Gestione dei sistemi informatizzati: modelli sanzionatori.

1. Introduzione.

La responsabilità penale connessa alla gestione dei sistemi informatizzati — con l'attenzione rivolta a strutture di recente applicazione, come i sistemi esperti — è tema vasto e complesso oltre che nuovo: ne tratterò dunque senza pretese di esaurire l'argomento[1].

La vastità e complessità del tema si apprezza considerando quali e quante variabili intervengano nella combinazione fra responsabilità penale e *management* dei sistemi informatizzati.

Innanzitutto con il termine di sistema informatizzato si identifica una struttura tecnica — destinata al trattamento automatico di dati — composta di alcuni elementi, senza riguardo alla sua maggiore o minore complessità: ci si dovrebbe perciò riferire contemporaneamente a sistemi di dimensioni modeste, come a sistemi più articolati, che ovviamente interessano in misura e per ragioni diverse il diritto penale[2].

In secondo luogo, esistono sistemi impiegati in attività innumerevoli e diverse fra loro — dall'organizzazione degli archivi burocratici,

[1] Questo lavoro riproduce, con ampie modifiche e revisioni, il testo della relazione presentata al IV Congresso Internazionale sul tema *Informatica e regolamentazioni giuridiche*, organizzato dalla Corte Suprema di Cassazione, Centro elettronico di documentazione, tenutosi a Roma dal 16 al 21 maggio 1988.

[2] Per maggior chiarezza, si paragonino un sistema utilizzato per diagnosticare una classe di malattie — rispetto al quale si presentano necessità di regolare l'attività e di proteggere l'accesso — ed un piccolo sistema casalingo utilizzato per archiviare ricette o registrare appuntamenti.

al controllo delle centrali nucleari, dalla diagnosi clinica alla contabilità — ciascuna delle quali può porre peculiari questioni di natura penale[3].

Inoltre, la gestione dei sistemi può assumere schemi organizzativi complessi (sino ad essere affidata in tutto o in parte a centri esterni all'ente od all'impresa) con una correlativa divisione di compiti tra diversi soggetti: si assiste in tali casi al fenomeno della frantumazione degli effetti giuridici dell'attività informatizzata, che rende arduo puntualizzare la responsabilità in capo ad un individuo determinato, sicché i danni prodotti tendono a divenire « anonimi »[4].

Si deve, quindi, tener conto della relazione variabile che esiste tra sistema ed impresa: l'attività dell'impresa si può risolvere integralmente in quella svolta dal sistema (quando sia diretta alla sola produzione dei servizi informatici) oppure il sistema può svolgere un'attività strumentale rispetto all'oggetto principale dell'impresa[5].

Infine, gli elaboratori (e dunque i sistemi) sono strumenti *prone to misuse*, secondo un efficace espressione anglosassone[6], ed, inoltre, criminologicamente versatili: cioè capaci di divenire oggetto o mezzo per la commissione di reati eterogenei: frodi, lesioni all'integrità fisica, violazioni tributarie, falsificazioni.

All'estensione del fenomeno si aggiunge la sua novità. Nell'ordinamento italiano, l'impiego dei sistemi informatici non è disciplinato da una specifica legislazione (extrapenale o penale): sicché la repressione delle condotte illecite resta ancorata alla normativa penale comune, come verrà considerato in seguito. La ricerca è poi resa difficoltosa dall'assenza di una casistica esauriente: manca un quadro completo e circostanziato delle evenienze che si possono realizzare attraverso un sistema informatizzato; difettando in particolare la documentazione relativa alle fattispecie di natura colposa, che potrebbero interessare la responsabilità della gestione[7].

[3] A. TRAVERSI, *Il diritto dell'informatica*, Milano, 1986, p. 169, distingue ad esempio ben tre livelli di utilizzazione dei sistemi informativi all'interno dell'impresa: sistema di base (o monofunzionale); sistema integrato o di controllo; sistema direzionale (nell'ambito dei quali colloca i sistemi esperti).

[4] L'argomento è ormai comune sia alla dottrina civilistica che alla dottrina penalistica, per una analisi ormai classica del tema: S. RODOTÀ, *Il problema della responsabilità civile*, Milano, 1967, p. 22.

[5] La dottrina civilistica si è recentemente dedicata alla trattazione del tema dei contratti c.d. di informatica, per tutti cfr.: AA.VV., *I contratti di informatica*, Milano, 1987, a cura di G. ALPA e V. ZENO ZENCOVICH; P. LA ROSA, *Lineamenti dei contratti di fornitura di computer services e di servizi informatici*, in *Informatica e situazioni giuridiche soggettive*, Napoli, 1986, 213.

[6] L'espressione è utilizzata anche nel Progetto per una legge contro la criminalità informatica elaborato in Australia, Tasmania, *Research paper on Computer Misuse.*

[7] Alcuni riferimenti in C. ROSSELLO, *La responsabilità da inadeguato funzionamento di programmi per elaboratore elettronico*, in *Computers e responsabilità civile*, Milano, 1985, 87 e in S. NYCUM, *Liability for Malfunction of a Computer Program, 7 Rutgers Computer Techn. L. Journ* (1979), p. 1. Rileva la totale mancanza di casistica significativa per i sistemi esperti A. ZOPPINI, *Commercializzazione dei sistemi esperti e responsabilità civile*, Atti IV Congresso, *Informatica e regolamentazioni giuridiche*, cit., III, 22, p. 8.

La situazione così delineata impone perciò di procedere con metodo empirico, ipotizzando prima gli accadimenti che possono realizzarsi nell'attività di un sistema e, poi, verificando in che termini ed a quale titolo possa scaturirne la responsabilità della gestione; anche se — è necessario precisare — in questa sede non si può che tentare un primo inquadramento della materia, senza tener conto di tutte le indicate variabili e senza svolgerne compiutamente le implicazioni.

2. Sistemi tradizionali e sistemi esperti.

Per « sistema informatico » si intende usualmente una struttura per l'elaborazione automatica di dati costituita da un'unità centrale e da componenti periferiche. Nella legislazione statunitense rivolta alla repressione della criminalità informatica, il *computer system* è definito come *a set of related, connected or non connected, computer equipment, devices and software*[8]. La nozione di sistema risulta perciò complementare a quella di *computer* e risente della problematica sorta, in sede di elaborazione della normativa penale, per definire quest'ultimo termine. La questione tecnico-definitoria — almeno negli Stati Uniti — ha avuto principalmente due obiettivi: individuare una nozione di elaboratore comprensiva e duttile, che non rimanesse fossilizzata alla tecnologia esistente e potesse adattarsi anche a strumenti più evoluti, e nel contempo riduttiva, sicché potessero escludersi dall'area di operatività della legislazione, strumenti come le agendine automatiche, i forni a micro-onde e gli orologi digitali, per cui appariva inopportuna un'estesa e severa tutela penale[9]. Nella più recente legislazione statunitense, il *computer* è stato definito come: « *an electronic, magnetic, optical, electrochemical, or other speed data processing device performing logical, arithmetic or storage functions* » « *but such term does not include an authomated typewriter or typesetter, a portable hand calculator, or other similar devices* »[10].

[8] Ariz. Crim. Code, par. 13.2301.E.6; Colo Rev. Stat. 18-5.5-101; Fla. Stat. Ann., 815.03(5); Mich. Stat. Ann. 28529 (2)-(6); N.M. 3016 A-2F; N.C. Gen. Stat. 14-453 (6); R.I. 1152-1(C); Utah Crim. Code 16-702(2).

[9] Per un'analisi della problematica sorta negli Stati Uniti per la definizione del termine *computer*, cfr. G. Corrias Lucente, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in questa *Rivista*, 1987, parte prima p. 167, part. p. 174; J.B. Tompkins e L. Mar, *An Analysis of 1984 Federal Computer Provisions*, in *L. & Techn* (1985), p. 1, part. p. 8; L. Wharton, *Legislative Issues on Computer Crime, 21 Harvard J. on Legisl*, p. 239 (1984); A.M. Wagner, *The Challenge of Computer Crime, How should New York Respond?, 33 Buffalo L. Rev.*, p. 777 (1984).

[10] 18 USC par 1030. La definizione è introdotta dal *Counterfeit Access Device and Computer Fraud Act*, emanato nel 1984.

La definizione accolta nella legislazione federale, che pare circoscrivere in maniera adeguata alle esigenze della normativa penale la nozione di elaboratore, verrà seguita nel prosieguo di questo lavoro, in cui si ometterà ogni riferimento a sistemi di modeste dimensioni.

L'attività dei sistemi tradizionali è regolata dal programma: si può distinguere fra unità di controllo e sistema operativo (che nella maggior parte dei casi risiede nell'*hardware*) che contengono tutte le informazioni necessarie per l'attività della macchina e per l'elaborazione dei dati, e programma o *software*, che contiene il complesso di istruzioni necessarie per svolgere le operazioni. Tali istruzioni, incorporate in un supporto materiale, sono costituite da un algoritmo, tradotto, poi in linguaggio binario[11].

I sistemi informatici sono applicati in diversi settori: nell'impresa, nelle pubbliche amministrazioni o da enti privati con funzione di conservazione e di elaborazione di dati; si rivelano particolarmente utili nell'attività bancaria, per la tenuta della contabilità e per le proiezioni economiche.

Recentemente sono entrati in attività sistemi ancor più sofisticati, detti « esperti », perché destinati ad assistere nella soluzione di (e tendenzialmente a risolvere) quei « problemi complessi che normalmente richiederebbeo l'intervento di un esperto umano nel dominio in cui operano »[12].

Caratteristiche fondamentali di questi sistemi sono: emulare il ragionamento dell'esperto, spiegare e giustificare (attraverso il dialogo con l'utente) il proprio comportamento; sicché possono guidare persone poco esperte nell'esecuzione di procedure complesse, poco note o con frequenti eccezioni. Una definizione più specifica dei sistemi esperti è resa difficoltosa dalla circostanza che esistono differenze rilevanti fra i diversi sistemi a seconda del settore in cui operano e della funzione che sono destinati a svolgere; così ad esempio un sistema che controlla in tempo reale un impianto industriale si distingue da un altro, che pianifica la produzione di beni.

[11] La letteratura tecnica sul tema è cospicua. Per ulteriori riferimenti bibliografici può rinviarsi agli autori giuridici che hanno trattato l'argomento, fra cui: A. TRAVERSI, *op. cit.*, p. 131; AA.VV., *La tutela giuridica del software*, a cura di G. ALPA, Milano, 1984; GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984, p. 21, ss.; AA.VV., *I programi per elaboratore elettronico. Tutela degli utenti e delle Software Houses*, a cura di L. RUSSI e V. ZENO-ZENCOVICH, Milano, 1988; S. PASCALINO, *Elementi costitutivi di un sistema informatico*, in *Informatica e situazioni giuridiche*, cit., p. 189; S. PASTORE, *Software e riproduzioni abusive, diritto d'autore, pirateria e tutela penale*, *ibidem*, p. 199; G. GHIDINI, *La proteggibilità dei programmi elettronici e dei relativi manuali applicativi quali opere dell'ingegno di carattere creativo*, in questa *Rivista*, 1985, 252; R. BORRUSO, *Computer e diritto*, Tomo I, *Analisi giuridica del computer*, Milano, 1988, p. 31.

[12] S. CAMMARATA, *Sistemi esperti, teorie, metodi, strumenti tecnici*, Milano, 1987, p. 5. Analoghe definizioni in R. BORRUSO, *op. cit.*, p. 214; A. ZOPPINI, *op. cit.*, p. 2; C. BERNARD, *Les systemes experts d'aide à la decision juridique: quelle aide pour quelle decision*, in Atti IV Congresso, *Informatica e regolamentazioni*, cit., X, 28, p. 2.

I sistemi esperti si differenziano da quelli tradizionali sia per l'architettura delle componenti tecniche, sia per l'aspetto funzionale. Si suole riassumere questa distinzione con l'affermare che la tecnologia dei sistemi tradizionali è *data based*, mentre i sistemi esperti sono *knowledge based*. La rilevata differenza consegue alla diversa ideologia o tecnica di programmazione che viene utilizzata[13]. Un sistema esperto, strutturalmente considerato, consta di una base di conoscenza, di un motore inferenziale, di una base di dati, di un'interfaccia. La base di conoscenza (*Long Term Memory*) è un complesso di regole e concetti propri di un dominio e rappresentati in forma dichiarativa e disaggregata. È costruita attraverso la collaborazione di due figure: l'esperto del settore (che apporta il complesso di regole di esperienze e di conoscenze professionali indispensabili per la soluzione di problemi specifici e complessi) e l'ingegnere della conoscenza, che pur non avendo conoscenze specialistiche della materia, rappresenta formalisticamente le regole di esperienza e le traduce in realizzazioni concrete. L'acquisizione della conoscenza si fonda perciò su basi empiriche. Il motore inferenziale (collocato nell'*hardware*) consente di svolgere, sulla base della deduzione logica, ragionamenti generali in stile precettivo. La base dei fatti (*Short Term memory*) contiene invece i dati iniziali del problema e si arricchisce dei dati progressivamente dimostrati sino alle conclusioni[14]. L'acquisizione della conoscenza si fonda perciò su basi empiriche. Mentre i sistemi tradizionali sono programmati in modo deterministico ad elborare dati alfanumerici, i sistemi esperti non sono rigidamente deterministici, accettano un margine d'incertezza nella soluzione delle questioni e possono proporre anche alternative[15]; non hanno, tuttavia, capacità di applicazioni generali (*General Solving Problem*) — la diagnostica clinica ad esempio — ma operano in uno specifico settore per la soluzione di problemi determinati: diagnosi di una determinata classe di malattie[16]. La panoramica delle applicazioni dei si-

[13] S. CAMMARATA, *op. cit.*, p. 70 ss. Per tracciare la differenza di fondo A. ZOPPINI, *op. cit.*, p. 2, considera come i sistemi tradizionali siano caratterizzati da una dimensione informativo/descrittiva mentre ai sistemi esperti sia propria una dimensione interpretativo/inferenziale.

[14] S. CAMMARATA, *op. cit.*, p. 74, che dedica particolare attenzione alla base di conoscenza raccolta nei c.d. *shells* (o gusci) (part. p. 179); A. ZOPPINI, *op. cit.*, p. 3; R. BORRUSO, *op. cit.*, p. 217; ai quali si rinvia anche per ulteriori precisazioni tecniche e bibliografiche.

[15] S. CAMMARATA, *op. cit.*, p. 70; G. CARIDI, *La rappresentazione della conoscenza giuridica per i sistemi esperti*, Atti IV Congresso, *Informatica e regolamentazioni*, cit., X, 4, p. 11; E. FAMELI, F. NANNUCCI, *I sistemi esperti nel diritto, strumenti e metodi di sviluppo*, *ibidem*, X, 10, p. 1 ss.

[16] In merito ai limiti dei sistemi esperti: S. CAMMARATA, *op. cit.*, p. 69; svolge osservazioni interessanti di natura generale sulla capacità dei sistemi esperti: S. CIPRI, *L'evoluzione dell'informatica come veicolo di comunicazione*, Atti IV Congresso, *cit.*, X, 17, p. 3 ss.

stemi esperti è comunque vasta e comprende: l'ingegneria (manutenzione e riparazione di impianti, gestione di centrali nucleari); i trasporti (pianificazione dei voli o dei carichi aerei, assistenza al controllo del traffico aeroportuale); le imprese bancarie (concessione dei fidi, assistenza nell'assunzione di rischi, pianificazione degli investimenti); le industrie (pianificazione delle linee di produzione, controlli di qualità, preventivazione dei costi, robotica); la medicina (controlli ed esperimenti di ingegneria genetica, assistenza di pazienti sottoposti a terapie intensive, diagnosi di classi di malattie) ed anche l'informatica (sorveglianza e controllo di sistemi e *test* di componenti)[17].

Come si è rilevato, i sistemi esperti si differenziano dagli altri negli aspetti funzionali e strutturali, ciò che si riflette sul contenuto e sull'ampiezza degli obblighi di gestione, comportandone anche l'estensione. Non si modificano, invece, i criteri per la determinazione della responsabilità che restano invariati rispetto alla disciplina comune. Va, infatti, precisato che i sistemi esperti non sollevano ancora quella serie di questioni circa la responsabilità e l'imputazione della loro attività, che potrebbero, per contro porre più generali applicazioni delle intelligenze artificiali. Seppur creati nel corso di studi sulle I.A., i sistemi esperti non presentano alcuni dei caratteri salienti dell'intelligenza, come l'autonomia rispetto al pur sofisticato programma che li governa, la capacità di automatico apprendimento dall'esperienza, la libertà di determinazione[18]. Vale, dunque, per i sistemi esperti il « teorema di Tesler » secondo cui « l'intelligenza artificiale è tutto ciò che non abbiamo ancora fatto », sicché « non appena si riesce a programmare qualche funzione essenziale, immediatamente si smette di considerarla un ingrediente del vero pensiero. Il nucleo ineluttabile dell'intelligenza è sempre in quell'altra cosa che non si è ancora riusciti a programmare »[19]. Sarebbe perciò fuor di luogo, in relazione ai sistemi esperti — come per i sistemi tradizionali — qualunque interpretazione antropomorfica. Escludere che il si-

[17] A. MAZZETTI, *Applicazioni dei sistemi esperti*, Padova, 1987; S. CAMMARATA, *op. cit.*, p. 221. La descrizione di alcuni progetti o realizzazioni di sistemi esperti — con particolare riguardo alle applicazioni nel campo dell'informatica giudiziaria — è svolta da R. BORRUSO, *Computer e diritto*, tomo II, Milano, 1988, p. 84 ss.; M. ANDRETTA, M. LUGARESI, F. ZAMBON, M.G. LOSANO, N. NANNINI, *I linguaggi formali applicati alla rappresentazione di testi normativi: il progetto PROLEG*, Atti IV Congresso, cit., X, 2; L.E. ALLEN, C.S. SAXTON, *Automatic Generation of a legal expert system of sec. 7 (2) of the U.K. Data protection Act 1984*, *ibidem*, X, 14; C. MORDÀ, G. ROCCA, F. PIVA, *The Rule of Law and the Law of Rules*, *ibidem*, X, 16; D. BROWERS, M. SCHAUSS, *Consideration methodologiques sur les systemes d'aide à la decision juridique*, *ibidem*, X, 29; A. CAPPELLI, L. MORETTI, F. PAGNI, *Verso la costruzione di una base di conoscenza per un sistema di aiuto ad un esperto nel campo della radioprotezione*, *ibidem*, X, 22; ed in genere gli atti del citato Congesso, sessione X.

[18] Al riguardo: S. CAMMARATA, *op. cit.*, p. 6 ss.

[19] R.D. HOFSTADTER, *Godel, Escher, Bach*, Milano, 1984, p. 649.

stema costituisca un centro di imputazione di effetti distinto da quello delle persone che lo costruiscono, lo governano e lo impiegano non implica ancora l'affermazione che gli effetti pienamente rilevanti della sua attività debbano automaticamente imputarsi a quelle persone fisiche. Per riferire la responsabilità di tali conseguenze bisogna, infatti, procedere secondo i criteri tipici stabiliti dal diritto penale; criteri d'imputazione che, in astratto o nelle concrete applicazioni possono condurre ad escludere la responsabilità penale delle persone che a prima vista paiono gli artefici del sistema.

3. Responsabilità penali della gestione.

Compete alla gestione: tenere attivo il sistema, mantenerlo in efficienza e preservarne l'integrità, attraverso l'adozione di livelli ottimali di sicurezza e di standard di controlli, nonché pratiche di opportuna manutenzione, che consentano di prevenire l'inserzione di estranei nel sistema od il suo difettoso funzionamento e di eliminare o ridurre le conseguenze degli abusi verificatisi. Il concreto contenuto di tali obblighi varia ovviamente in funzione del tipo e della complessità del sistema gestito.

La violazione degli obblighi della gestione dei sistemi non integra, in se considerata, alcun illecito penale mancando, nel nostro ordinamento, norme sanzionatorie specifiche. Alla stregua dei principi che regolano il sistema penale, può divenire complesso puntualizzare la responsabilità in capo ai preposti alla gestione, anche nel caso in cui la violazione degli obblighi inerenti la gestione stessa sia collegata ad un evento lesivo previsto da una fattispecie incriminatrice (ad esempio allorché all'impropria manutenzione del sistema consegua un suo inadeguato funzionamento produttivo di conseguenze — come morte o lesioni — penalmente rilevanti). Prescindendo dalla problematica delle fattispecie causalmente orientate, cui di seguito si farà cenno[20], va rilevato che i preposti alla gestione rispondono in sede penale dei fatti (previsti come reato) che abbiano direttamente e dolosamente commesso attraverso il sistema. In tale ambito acquistano rilievo le questioni relative alla criminalità informatica e cioè a quella serie di modelli comportamentali — alcuni dei quali non integranti reato — che possono essere realizzati attraverso gli elaboratori (od i relativi sistemi) ovvero in danno di essi e delle loro componenti.

La problematica di ordine giuridico posta dai c.d. *Computer Crimes* non esaurisce però l'area d'interesse penalistico relativa ai sistemi informatizzati, che va estesa anche a tutti i reati che, pur non rientrando in questa specifica tipologia, si possono realizzare attraverso un sistema.

[20] *Infra*, par. 3, lett. *b*).

a) *Per illeciti di natura dolosa.*

L'analisi pragmatica ha consentito di ricostruire e classificare le tipologie di *Computer Crimes*: ci si riferisce così all'accesso abusivo, all'uso non autorizzato dell'elaboratore, alla sottrazione ed al danneggiamento di dati e programmi (o di componenti fisiche del sistema), all'alterazione del loro contenuto, ed, infine, alle frodi informatiche: evenienze tutte che ledono o mettono in pericolo l'efficienza e l'integrità del sistema[21]. Va subito rilevato che non esistono, rispetto a questi comportamenti, strumenti tecnici di sicura prevenzione. Si riscontrano, inoltre, diverse lacune sul piano della tutela penale. Converrà partitamente esaminare i diversi modelli degli illeciti in questione.

A) È considerato accesso abusivo, il collegamento o l'inserzione nel sistema da parte di una persona non autorizzata, oppure da parte di un soggetto che superi i limiti dell'autorizzazione ottenuta. L'accesso abusivo riveste una duplice valenza: può presentarsi come un comportamento prodromico alla commissione di un altro illecito, ovvero come un fenomeno fine a se stesso determinato da scopi ludici o luddistici. Qualunque sia la finalità che lo sorregge, tale comportamento mette in pericolo la sicurezza del sistema e gli interessi correlati al suo impiego, sia quelli di natura patrimoniale, sia quelli relativi alla riservatezza, ovvero all'incolumità fisica[22].

Di fronte alla potenzialità lesiva dei fatti di accesso abusivo, si riscontra in Italia l'assenza di una adeguata normativa sanzionatoria[23]. L'elevato coefficiente di pericolosità di questi comportamenti — e nel contempo l'inadeguatezza di sanzioni di natura extrapenale — potrebbero consigliare l'introduzione di una specifica fattispecie incriminatrice, che sanzioni l'accesso abusivo o le sue più gravi mani-

[21] Sul tema della criminalità informatica, con ampi riferimenti comparatistici: C. SARZANA, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1984, II, 21; ID., *Sviluppo tecnologico e criminalità*, in *Informatica ed evoluzione dell'attività giuridica*, Firenze, 1985, p. 159; L. PICOTTI, *La falsificazione dei dati informatici*, in questa *Rivista*, 1985, p. 939; G. CORRIAS LUCENTE, *op. cit.*, I parte (p. 167), II parte (p. 519); inoltre gli atti del Convegno *La Criminalità informatica, prevenzione e repressione*, organizzato dal CED, Roma, 4-6 dicembre 1986; F. MUCCIARELLI, *Computer (Disciplina giuridica del) nel diritto penale*, voce, *Dig. IV, Disc. pen.*, vol. II, Torino, 1988, p. 373.

[22] Sul fenomeno: D.B. PARKER, *Crime by Computer*, New York, 1976, p. 276; R.D. NORMAN, *Computer Insecurity*, Londra, 1983, p. 247 ss.; M.D. SCOTT, *Computer Law*, New York, 1984, par. 8.4; U. SIEBER, *The International Handbook on Computer Crime*, New York, 1986, p. 19; A.M. WAGNER, *op. cit.*, p. 1; G. CORRIAS LUCENTE, *op. cit.*, p. 179 ss.; C. SARZANA, *Informatica e diritto penale. Problemi prospettive ed aree di ricerca*, relazione al Convegno: *La criminalità informatica*, cit., p. 14.

[23] Non risulta configurabile, infatti, l'ipotesi prevista dall'art. 617 cod. pen. Per una più estesa analisi: G. CORRIAS LUCENTE, *op. cit.*, p. 191, ss.

festazioni, delimitandole attraverso una specificazione della condotta o la previsione del dolo specifico[24].

B) Rilevano quindi fatti quali l'uso non autorizzato dell'elaboratore (denominato anche furto di tempo) che può essere determinato da intenti meramente ludici od economici — come nei frequenti casi di dipendenti che organizzano un'autonoma attività imprenditoriale tramite l'elaboratore della loro ditta)[25]. Tali fattispecie non integrano nell'ordinamento italiano alcuna ipotesi di reato, eccettuate alcune estreme manifestazioni di questo comportamento, in cui si impegna la capacità dell'elaboratore sino a renderlo indisponibile al titolare, che potrebbero realizzare (nel ricorso degli altri presupposti del reato) un fatto di peculato per distrazione dell'elaboratore stesso[26].

Fuori da questi casi limite, il furto di tempo, pur essendo economicamente dannoso, non presenta connotati tali da meritare sanzione penale; va al riguardo considerato che si presenta analogo ad altri comportamenti (come l'uso di veicoli o di macchine da scrivere dell'ufficio per scopi personali) che non sono penalmente sanzionati nell'ordinamento italiano.

C) Anche la tutela dei dati e dei programmi incontra diversi limiti nel diritto positivo, in particolare per quanto riguarda il valore economico del contenuto. I reati di furto e danneggiamento, com'è noto, hanno ad oggetto beni materiali: la sanzione penale è perciò applicabile alle condotte lesive tipiche, che si incentrino su di un supporto fisico. La necessità che la modifica della situazione tutelata avvenga in modo fisicamente tangibile e concerna un bene materiale induce ad

[24] Questa la strada seguita dalla più recente legislazione statunitense in materia. A livello federale è stato sanzionato penalmente l'accesso abusivo qualificato dall'intento di apprendere informazioni riservate in materia di difesa, politica estera od applicazioni di energia atomica; ovvero dall'intento di apprendere informazioni finanziarie; od ancora l'accesso abusivo cui sia conseguita l'apprensione, distruzione o rivelazione di dati contenuti in elaborati operanti per il Governo (18 USC par. 1030 *a*) (1-3) il cui testo è riportato in G. CORRIAS LUCENTE, *op. cit.*, p. 187, cfr. anche per l'analisi delle fattispecie incriminatrici introdotte dai singoli stati americani.

[25] D. PELLEGRINI, *Uso non autorizzato del computer: limiti e prospettive della tutela penale*, in questa *Rivista*, 1987, 289; G. CORRIAS LUCENTE, *op. cit.*, p. 182; F. MUCCIARELLI, *op. cit.*, p. 378; C. SARZANA, *Note*, cit., p. 28. Nella letteratura straniera: J.B. TOMPKINS e L.A. MAR, *op. cit.*, p. 9; L. WHARTON, *op. cit.*, p. 252; L. MENNELLY, *op. cit.*, p. 566, con riferimento alla giurisprudenza statunitense; J.P. SPREUTELS, *Les infractions liées à l'informatique en droit belge*, in *Rev. dr. pén. et chrim.*, 1985, p. 387; S. SCHOLBERG, *Computer and Penal Legislation*, Oslo, 1983, p. 25; K. TIEDEMANN, *Criminalità da computer*, in *Pol. dir.*, 1984, p. 613, part. p. 621; U. SIEBER, *op. cit.*, p. 81, cui si rinvia per ulteriori riferimenti.

[26] In tal senso, D. PELLEGRINI, *op. cit.*, p. 294 ss.; G. CORRIAS LUCENTE, *op. cit.*, p. 196. Si tratta, invero, di un'ipotesi di furto di servizi, fattispecie che non è sanzionata attraverso le disposizioni sul furto e sull'appropriazione indebita. Sulla carenza di tutela delle attività produttrici di servizi: F. SGUBBI, *Patrimonio (Reati)*, in *Enc. dir.*, vol. XXXII, Milano, 1982, p. 331, spec. p. 360; P. NUVOLONE, *Antinomie fossili e derivazioni del codice penale italiano*, in *Trent'anni di diritto e procedura penale*, vol. I, Padova, 1969, p. 714.

escludere che l'apprensione o la cancellazione delle sole informazioni in cui i dati e i programmi consistono siano attualmente punibili a titolo di furto o di danneggiamento[27]. Va però rilevato che la lacuna di tutela così riscontrabile non appare ad un'attenta analisi del tutto ingiustificata, atteso che i beni cui si ha riguardo possono contenere oltre che informazioni di considerevole valore economico anche informazioni prive di rilevanza patrimoniale (come avviene per i dati notori) sicché le condotte che su di essi incidono possono risultare anche innocue. Introdurre fattispecie incriminatrici per proteggere ogni e qualsiasi dato e programma rispetto a condotte di apprensione e cancellazione comporterebbe due effetti ingiustificati: estenderebbe, da un lato, la tutela di questi beni oltre i limiti di quella assicurata alle informazioni conservate in maniera tradizionale, e dall'altro sottoporrebbe ad un trattamento indifferenziato beni di valore diverso e condotte di differente capacità lesiva[28].

D) A risultati insoddisfacenti si perviene inoltre, nel settore della tutela penale della veridicità dei dati. Nell'attuale sistema penale, le fattispecie incriminatrici della falsità in atti, sono, invero, ancorate ad una nozione di documento caratterizzata dalla forma scritta, dall'incorporazione in carta e dalla sottoscrizione (o quantomento dalla riconoscibilità dell'autore) non riscontrabili nel documento informatico. È sufficiente al riguardo, considerare che i dati sono conservati nella memoria sotto forma di impulsi elettronici e che gli elaborati, anche se conservati in carta, spesso non vengono sottoscritti, né è possibile attraverso essi risalire all'operatore che ha memorizzato l'informazione[29].

[27] F. MUCCIARELLI, *op. cit.*, p. 379; G. CORRIAS LUCENTE, *op. cit.*, 519; C. SARZANA, *Note cit.*, p. 26; A. TRAVESI, *op. cit.*, p. 193; M.P. LUCAS DE LEYSSAC, *Il furto d'informazione*, in questa *Rivista*, 1985, p. 625; L. MENNELLY, *op. cit.*, p. 577; G. THACKERAY, *op. cit.*, p. 248; J.T. SOMA, *op. cit.*, p. 282; P. CATALA, *Les transformations du droit pénal de l'informatique*, in *Emergence du droit de l'informatique*, Parigi, 1983, p. 264; A. MANNA, *Aspetti problematici della c.d. criminalità informatica nei paesi francofoni*, in questa *Rivista*, 1987, p. 503.

[28] Un'eccessiva estensione della tutela penale delle informazioni archiviate in forma elettronica pare discendere dalla recente legislazione degli stati americani. In alcuni, infatti, si è stabilito che *property includes computer programs or data* (Il. Crim. Code, sec. 15-1; V Code, par. 18.2-98.1; Tenn. Code Ann., par. 39-3, 1403h) determinando l'estensione di tutte le fattispecie incriminatrici a tutela della property anche ai dati ed ai programmi. Altrove, e con gli stessi effetti, si è disposto che *For the purpose of this section property means financial instruments, informations, including electronically produced data, computer software and programs in either machine or readable form, and anything of value, tangible or intangible (Ariz. Crim. Code 13-2301 E8; Cal. Pen. Code par. 502 (a) (7); Colo Rev. Sta. 18.5.-101 (8); Mich. Sta. Ann. par. 28.5 29 (3) (1); N.C. Gen. Stat. Ann. par. 14-453 (8); R.I. 11.52.1 (E); Utah Crim. Code par. 76-6-702 (5); GA Code par. 16-9-92 (7).*

[29] L. PICOTTI, *La falsificazione dei dati informatici*, cit., p. 939; F. MUCCIARELLI, *op. cit.*, p. 380; C.G. CIMARELLA, *La tutela penale del documento elettronico*, in questa *Rivista*, 1986, p. 949; C. SARZANA, *Note*, cit., p. 28; G. MARINI, *Condotte di alterazione del reale aventi ad oggetto nastri e supporti magnetici e diritto penale*, in *Riv. dir. proc. pen.*, 1986, p. 382, anche in *Informatica e situazioni*, cit., p. 159; G. CORRIAS LUCENTE, *op. cit.*, p. 535; tutti con ampi riferimenti alla dottrina straniera.

Si rende perciò opportuno apprestare una tutela più incisiva ed estesa della veridicità dei dati, atteso che costituiscono una forma di memorizzazione di atti giuridicamente rilevanti. Tuttavia, la formulazione di un'eventuale fattispecie incriminatrice e la relativa sfera di operatività meritano attenta valutazione: segnatamente appare necessario effettuare una selezione accurata dei dati, oggetto della tutela penale, poiché potrebbe risultare inopportuno garantire la veridicità di tutte le informazioni conservate in forma elettronica, senza considerare la natura (atto pubblico, certificazione amministrativa o scrittura privata) dell'atto in cui sono destinate ad incorporarsi[30].

E) Nell'ordinamento italiano anche talune ipotesi di frodi informatiche sfuggono alle maglie della vigente normativa penale. Per l'integrazione del reato di truffa è, infatti, necessaria l'induzione in errore di una persona, e tale elemento della fattispecie non sussiste quando l'elaboratore provvede ad eseguire una disposizione patrimoniale, preordinata nel programma, a seguito dell'inserzione di falsi dati[31]. Per ovviare a tali lacune si è tentata la qualificazione del fatto a titolo di furto con mezzi fraudolenti: siffatta figura di reto non appare, però, configurabile allorché il profitto sia conseguito dall'agente attraverso la mediazione di un atto giuridico (ad esempio un ordine di pagamento o l'iscrizione a credito delle somme) che esclude l'usurpazione unilaterale in cui il furto consiste[32].

Rispetto ad illeciti di questa fisionomia, l'opportunità di sanzione penale riulta, però evidente, considerato che si profilano come ipotesi

[30] Nella legislazione federale statunitense si è ritenuto opportuno sanzionare la falsificazione di alcune categorie di dati; a livello statale si è invece optato per una tutela indifferenziata della veridicità dei dati e dei programmi, cfr. la normativa riportata in nota a G. CORRIAS LUCENTE, *op. cit.*, p. 533.

[31] Descrivono le diverse tecniche di frodi informatiche: K. TIEDEMANN, *op. cit.*, p. 619, L. TRIA, *Osservazioni in tema di reati elettronici*, in *Arch. pen.*, 1984, p. 283, part. p. 286; R.D. NORMAN, *op. cit.*, p. 72; J.K. TABER, *A Survey of Computer Crimes studies, in 2 Computer L.J.*, p. 311 (1980); U.S. DEPARTMENT OF JUSTICE, *Computer Crime, Criminal Justice Resource Manual*, Washington, 1980, p.c.; D.B. PARKER, *Crime*, cit., p. 84; ID., *The computer Criminal: Motivations and Modus Operandi*, Relazione al Convegno CED, *cit.*, p. 2 ss.; M.D. SCOTT, *op. cit.*, par. 8.9; U. SIBER, *op. cit.*, p. 6. Quanto alla rilevanza penale delle diverse tipologie di frodi, nel senso del testo: L. PICOTTI, *La falsificazione*, cit., p. 958; A. TRAVERSI, *op. cit.*, p. 192; G. CORRIAS LUCENTE, *op. cit.*, p. 541; F. MUCCIARELLI, *op. cit.*, p. 377 e 380. Ritengono configurabile il reato di truffa: C. SARZANA, *Reati resi possibili*, cit., p. 22; ID., *Informatica e diritto penale. Problemi prospettive ed aree di ricerca*, Convegno CED, cit., p. 21; U. PIOLETTI, *Truffa*, in *Noviss. Dig. it.* (App.), vol. VII, Torino, 1987, p. 907 (cfr. p. 912).

[32] L'ipotesi della configurabilità del furto aggravato dal mezzo fraudolento è stata vagliata soprattutto con riguardo a prelievi indebiti tramite il sistema Bancomat e ad alcuni casi di trasferimento elettronico di fondi. Qualificano in tal modo le frodi informatiche: F. MUCCIARELLI, *I computer Crimes nel disegno di legge 1657/1984*, in *Riv. it. dir. proc. pen.*, 1984, 785; G. MARINI, *op. cit.*, p. 386; L. TRIA, *op. cit.*, p. 390, *contra* G. CORRIAS LUCENTE, *op. cit.*, p. 544.

concretamente dannose e presentano aspetti rilevanti di analogia con fattispecie di reati esistenti (come la truffa).

F) *Nulla quaestio*, invece, per la tutela delle componenti fisiche di un sistema informatizzato, che nell'ordinamento italiano sono attualmente protette ad un duplice livello: attraverso il reato generale di danneggiamento di cose (art. 635 cod. pen.) e dalla fattispecie più grave, per il profilo lesivo e sanzionatorio, dell'attentato agli impianti di elaborazione di dati (art. 420 cod. pen.)[33].

L'incerto e lacunoso quadro di tutela che risulta dalla sintesi svolta incide indubbiamente sull'estensione obiettiva della responsabilità dei preposti alla gestione. Va, infatti, rilevato che essi sono agevolati nella commissione delle ipotesi appena considerate — avendo una conoscenza diretta e completa delle capacità del sistema gestito, cui si accompagna un'illimitata facoltà di accesso e di sfruttamento delle sue potenzialità — tanto che si giustificherebbe a loro carico un aggravamento della pena prevista per gli illeciti commessi.

Oltre alle fattispecie ora richiamate, attraverso un sistema si possono commettere reati diversi; ad esempio (e senza pretesa di esaurire l'elenco) illeciti fiscali, ove sia destinato a svolgere funzioni connesse con gli obblighi tributari, delitti contro la persona (p.e. con l'alterazione dei dati relativi alla diagnosi od alla terapia cui è sottoposto un paziente) od ancora delitti contro l'incolumità pubblica.

È ovvia considerazione che i preposti alla gestione rispondano dei reati che abbiano dolosamente e direttamente commesso, siccome dei reati alla cui realizzazione abbiano consapevolmente partecipato, secondo la disciplina del concorso di persone nel reato.

Problematica risulta, invece, la soluzione del caso in cui alla violazione colposa delle regole di gestione dei sistemi segua la commissione di un illecito doloso da parte di terzi; salva la responsabilità dell'autore del fatto, si può porre la questione se, ed a quale titolo, ne rispondano anche i preposti alla gestione.

Divergenti sono le soluzioni dogmatiche proposte da cui, peraltro, scaturiscono diverse conseguenze circa il contenuto della fattispecie di partecipazione colposa al reato doloso, variandone i termini essenziali, quali l'identificazione del titolo di responsabilità, delle figure di reato con esso compatibili, della portata del nesso eziologico — che necessariamente deve intercorrere fra la condotta colposa e l'illecito del terzo — ed infine dei criteri che presiedono all'individuazione della colpa.

[33] Sul tema: L. PICOTTI, *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione di dati*, in questa *Rivista*, 1986, p. 969; C. RAPISARDA, nota a G.I., Firenze, 27 maggio 1986, Pasqui, *Foro it.*, 1986, II, p. 359.

Va rilevato che la prevalente dottrina esclude — alla luce dell'inquadramento dogmatico e della disciplina normativa della fattispecie concorsuale — la configurabilità del concorso colposo nel reato doloso[34]. Di recente si è proposto di considerare l'art. 113 cod. pen. quale « norma di copertura del titolo di responsabilità colposa in ipotesi di cooperazione nelle quali convergono anche contributi colposi », richiedendosi di apprezzare l'atteggiamento colposo, non solo in termini di prevedibilità ed evitabilità dell'evento finale, ma anche secondo il criterio della prevedibilità ed evitabilità dell'altrui comportamento illecito[34-bis].

L'orientamento che ravvisa una forma di responsabilità per titolo autonomo, circoscrive, invece, la punibilità alle fattispecie causalmente orientate, rispetto alle quali la condotta colposa appare dotata di autonoma tipicità.

Al fine di ricostruire il fondamento della colpa in termini compatibili col principio di autoresponsabilità penale, si limita inoltre la responsabilità alle violazioni di determinati obblighi di garanzia, ovvero si attribuisce rilievo al criterio dell'affidamento, nell'individuazione della colpa, sì da considerare la violazione di quei soli doveri di diligenza che rispondono allo specifico scopo di evitare le aggressioni dolose di terzi[35].

Si tratta, indubbiamente, di ipotesi concrete di secondario rilievo, che, tuttavia, presentano aspetti d'interesse non solo teorico, quando l'attività del sistema coinvolga beni di essenziale rilievo.

b) *Per illeciti di natura colposa.*

Una serie di esempi, frutto delle ipotesi di alcuni studiosi o tratti dalla cronaca giornalistica, consente di individuare il settore della re-

[34] La questione appare controversa e si presenta come uno dei principali nodi dogmatici in tema di concorso di persone nel reato. Escludono, sulla base di considerazioni diverse, la configurabilità del concorso colposo nel delitto doloso: F. ANTOLISEI, *Manuale di diritto penale, parte gener.*, Milano, 1982, p. 507; A.R. LATAGLIATA, *Concorso di persone nel reato (dir. pen.)*, in *Enc. dir.*, vol. III, Milano, 1961, p. 582; G. FIANDACA, E. MUSCO, *Diritto penale, parte gener.*, Bologna, 1985, p. 267; F. ALBEGGIANI, *I reati di agevolazione colposa*, Milano, 1983, p. 208; M. GALLO, *Lineamenti di una teoria sul concorso di persone nel reato*, Milano, 1957, p. 112, cui si rinvia per ogni altro riferimento. Ammettono la configurabilità del concorso a diverso titolo: F. MANTOVANI, *Diritto penale*, Padova, 1988, p. 507; C. PEDRAZZI, *Il concorso di persone nel reato*, Palermo, 1952, p. 82 ss.; A. PAGLIARO, *Principi di diritto penale*, Milano, 1987, p. 560. Per l'ipotesi in cui i preposti alla gestione abbiano, con la loro condotta omissiva colposa facilitato o consentito la commissione del reato da parte di terzi, cfr., *infra* 3, *b*), cui si rinvia anche per quanto concerne la problematica relativa alla definizione dell'attività informatica come attività pericolosa.

[34-bis] P. SEVERINO DI BENEDETTO, *La cooperazione nel delitto colposo*, Milano, 1988, p. 236 s. (cit. p. 238), cui si rinvia per ulteriori approfondimenti.

[35] G. FIANDACA, E. MUSCO, *op. cit.*, p. 268 s., 299. In merito alla rilevanza dell'art. 40 cpv. riguardo all'attività dei sistemi, *infra*, par. 3.b). Sul criterio dell'affidamento: F. ALBEGGIANI, *op. cit.*, p. 122 ss.

sponsabilità colposa nell'ambito dei sistemi informatici: si tratta dei casi di disastro aereo o ferroviario provocati da un errore del sistema che governa il traffico dei trasporti[36], della morte di un paziente per errori nella diagnosi o nella terapia controllate da un sistema informatizzato ed in genere di tutti gli eventi penalmente rilevanti, determinati da un inadeguato funzionamento del sistema.

Le diverse ipotesi devono essere distinte a seconda che l'inadeguato funzionamento tragga origine nella fase di programmazione od in quella di utilizzazione del sistema: in entrambi i casi, va ribadito che si pone un'identica problematica: pervenire all'individuazione della fonte (umana) dell'inadeguato funzionamento e valutarne il comportamento alla luce dei criteri tipici del diritto penale.

L'inadeguato funzionamento può, in primo luogo, trovar origine da un errore verificatosi nella fase di programmazione. Si impongono, allora, considerazioni di diverso ordine per le due categorie di sistemi informatizzati cui si ha riguardo. Può, innanzitutto tracciarsi una differenza di fondo: il sistema esperto è ritenuto difettoso quando non fornisce una conoscenza esatta, un programma tradizionale lo è quando non elabora i dati nel modo previsto[37]. Sotto il profilo strutturale, nei sistemi tradizionali, la *defaillance* può inerire al sistema operativo od al *software*, occorrerà allora far capo alla persona od al *pool* di persone che hanno contribuito alla relativa ideazione e costruzione, tenendo conto del fatto che il sistema operativo è nella maggior parte dei casi prodotto dalle *Hardware Houses* mentre gli altri programmi dalle *Software Houses*[38]. L'inadeguato funzionamento dei sistemi esperti, può, invece, originare da cause insiste nel motore inferenziale o nella base di conoscenza: in quest'ultimo caso il difetto può inerire il contenuto delle regole empiriche — e, dunque rientrare nel dominio dell'esperto — od alla loro formalizzazione, e cioè collocarsi nel settore proprio dell'ingegnere della conoscenza; peraltro il difetto può dipendere dall'interrelazione delle attività, ed essere imputabile ad entrambi[39].

L'accertamento delle distinte responsabilità appare, in ogni caso, complesso, sul piano tecnico e su quello giuridico. Sia sufficiente considerare che il programma è spesso frutto di un lavoro di *equipe*, nell'ambito del quale può risultare difficile discernere l'apporto e la responsabilità dei singoli. Può, inoltre, rilevarsi difficoltoso indivi-

[36] Gli esempi sono proposti da C. ROSSELLO, *op. cit.*, p. 88; S.H. NYCUM, *op. cit.*, p. 7.

[37] Constata tale differenza A. ZOPPINI, *op. cit.*, p. 6.

[38] Cfr. G. ALPA, *Responsabilità extracontrattuale ed elaboratore elettronico*, in questa *Rivista*, 1988, 387; ROSSELLO, *op. cit.*, con ampi riferimenti all'elaborazione dottrinaria statunitense e G. PONZANELLI, *op. cit.*, p. 70.

[39] A. ZOPPINI, *op. cit.*, p. 7 con particolare riguardo ai sistemi esperti.

duare la portata e la sede dell'errore nei casi in cui non sia reperibile una documentazione scritta che consenta di ricostruire il contenuto del programma. La complessa ricostruzione fattuale degli eventi (o dei danni) determinati dal *software* ha indotto a parlare infatti di produzione invisibile del danno (o dell'evento)[40]. Né si può sottacere quanto divenga complesso l'accertamento concreto della colpa, soprattutto rispetto a sistemi che presentano un grado elevato di incognite di funzionamento, la cui estensione ed i cui effetti possono risultare imprevedibili.

L'inadeguato funzionamento può inoltre verificarsi nella fase di utilizzazione dell'impianto e dipendere da un'inserzione di dati non corretti o dall'adozione di procedure imprecise da parte dell'operatore. In tal caso è la condotta di quest'ultimo a dover essere apprezzata in termini di colpa; salvo che le sue manchevolezze non conseguano all'imprecisione delle istruzioni o degli ordini ricevuti, allorché si potrebbe risalire alla responsabilità di chi ha fornito le istruzioni od ordinato l'attività, ed in ultima analisi dei preposti alla gestione del sistema.

L'erroneo funzionamento del sistema, produttivo in un evento penalmente rilevante, può infine collegarsi a carenze nello svolgimento dei compiti gestionali, relativi alla manutenzione, ai controlli ed alle misure di sicurezza dell'impianto, che costituiscano una violazione degli obblighi di perizia e di diligenza riferibili alla gestione, ed integrino perciò la colpa dei preposti alla gestione stessa.

Per valutare tali ipotesi si rende necessario distinguere: se la condotta colposa si sia realizzata in forma commissiva, attraverso un'azione, od in forma omissiva. Nel secondo caso occorre confrontare la fattispecie concreta non solo con la norma incriminatrice di parte speciale ma anche con il disposto dell'art. 40 cpv. cod. pen., che, com'è noto, disciplina la regola dell'equivalenza fra produzione dell'evento ed omesso impedimento dello stesso[41]. Tale norma, si è rilevato, da luogo ad un fenomeno di integrazione della fattispecie di parte speciale, che viene ad arricchirsi di elementi di specialità che non risultano immediatamente evidenziati nella relativa fattispecie incriminatrice[42].

Il tema della responsabilità per il reato commissivo mediante omissione si è imposto all'attenzione della dottrina proprio in relazione al settore degli eventi lesivi connessi alla moderna attività indu-

[40] G. ALPA, *op. cit.*, p. 390.

[41] I contributi dottrinali sul reato omissivo improprio e sul reato commissivo mediante omissione sono numerosi e tutti degni di rilievo, ci si consenta perciò di rinviare oltre che alla manualitstica, solo alla più recente letteratura monografica in argomento: G. FIANDACA, *Il reato commissivo mediante omissione*, Milano, 1979; F. SGUBBI, *Responsabilità penale per omesso impedimento dell'evento*, Padova, 1975; G. GRASSO, *Il reato omissivo improprio*, Milano, 1983.

[42] G. FIANDACA, *op. cit.*, p. 70.

striale, ove si è ravvisata « una delle applicazioni più attuali e più impegnative del meccanismo di tutela » incentrato sull'art. 40 cpv.[43].

Per quanto attiene ai limiti della rilevanza penale dell'omissione, fra cui assume un ruolo centrale quello che l'art. 40 cpv. definisce l'obbligo giuridico di impedire l'evento, è in corso una profonda riflessione da parte della recente dottrina che ha sottoposto ad analisi critica i *topoi* della disciplina sinora individuati. Può, per quanto interessa, precisarsi che la gestione di fonti di pericolo è stata costantemente — seppur con giustificazioni profondamente diverse — ricompresa tra le situazioni tipiche in cui opera la regola dell'equivalenza. Ciò vale per la teorica che afferma la necessaria derivazione formale dell'obbligo di impedire l'evento, che inserisce nella terna delle fonti dell'obbligo anche il fare pericoloso precedente[44], ancorché si sia correttamente rilevato che in tal modo l'indirizzo menzionato entra in contraddizione con se stesso[45]. Ma anche nell'ambito delle più moderne elaborazioni, che integrano o sostituiscono la concezione formale con criteri contenutistico-sostanziali desunti dalla legge penale, acquista centrale rilievo la gestione delle fonti di pericolo. L'operare della regola fissata dall'art. 40 cpv. è, allora, ricollegato all'esistenza di un obbligo di garanzia, che incomba sul soggetto (il c.d. garante) e, in tale categoria di obblighi si ricomprendono anche quelli di protezione connessi appunto alla gestione delle fonti di pericolo[46].

Per quanto riguarda lo specifico argomento, l'assenza di regolamentazione legislativa fa si che non esistano, in capo ai preposti alla gestione dei sistemi, obblighi di derivazione formale validi ai sensi dell'art. 40 cpv. cod. pen.; ciò non toglie che obblighi di fonte legislativa riguardino espressamente alcune delle attività informatizzate (ad esempio, le centrali nucleari, gli ospedali) e perciò possano sussistere a titolo derivativo in capo alla gestione dei sistemi.

All'individuazione di una posizione di garanzia nei confronti del *management* dei sistemi potrebbe, dunque, addivenirsi a patto di riconoscere che il sistema informatizzato rappresenti una fonte di pericoli o, comunque svolga un'attività pericolosa. Non va però trascurato come appaia tutt'altro che scontata l'identificazione dell'attività informatizzata con l'attività pericolosa. Nell'ambito dell'elaborazione della responsabilità aquiliana si è, al riguardo, constatata la difficoltà di considerare tale l'elaborazione elettronica, concludendosi che « semmai può essere pericolosa l'attività che (avvalendosi

[43] *Ibidem*, p. 132; F. SGUBBI, *op. cit.*, p. 136.

[44] In tal senso F. ANTOLISEI, *op. cit.*, p. 217.

[45] G. FIANDACA, E. MUSCO, *Diritto penale, parte gener.*, cit., p. 335.

[46] G. FIANDACA, *op. cit.*; F. SGUBBI, *op. cit.*; G. GRASSO, *op. cit.*, il quale, segue un orientamento parzialmente diverso, ed inserisco tra le fonti legislative degli obblighi di garanzia anche l'art. 2050 cod. civ. (p. 320) così riferendosi a tutte le attività pericolose.

dell'elaborazione elettronica) ha comunque effetti di creazione del rischio, e li avrebbe nella stessa intensità e misura anche se fosse affidata all'azione meccanica o umana »[47].

I connotati dell'attività di elaborazione automatica di dati — soprattutto se affidata a sistemi esperti — devono, dunque, esser attentamente ricostruiti, attraverso un'analisi del problema che abbia riguardo non solo alle caratteristiche generali che i sistemi presentano, ma anche e soprattutto alle peculiari caratteristiche di sistemi determinati, adibiti allo svolgimento di precise funzioni ed attività. Per inciso va rilevato come nello stabilire quale disciplina giuridica applicare al caso concreto — se quella relativa ai reati omissivi impropri o quella delle fattispecie incriminatrici di parte speciale — rilevi la problematica demarcazione fra azione ed omissione: e che in alcuni dei casi prospettati potrebbe dubitarsi se la gestione risponda per aver tenuto attivo il sistema oppure per non avere effettuato manutenzione e controlli. Potrebbero cioè riproporsi, in relazione ai sistemi informatizzati, questioni analoghe a quelle sollevate in tema di circolazione stradale. Sussistono, tuttavia, differenze rilevanti fra le due ipotesi: l'autista imprime i movimenti e la direzione della vettura attraverso un controllo ed un'attività costanti; i sistemi informatizzati funzionano a prescindere da questa stretta identificazione con un controllo ed attività umane.

4. Responsabilità nella gestione di banche dati.

Premesso che le questioni già sorte per i sistemi tradizionali, si ripropongono anche per i sistemi esperti in quanto trattano masse di dati personali, può rilevarsi che nell'ordinamento italiano non è stata sino ad oggi introdotta una regolamentazione legislativa delle banche di dati, per quanto la loro attività sia risultata pericolosa per l'interesse alla riservatezza tutelato dal diritto positivo[48]. L'esigenza

[47] G. Alpa, *op. cit.*, p. 390.

[48] La dottrina italiana ha rivolto grande attenzione al tema delle banche di dati e della tutela della riservatezza; fra i molti contributi possono segnalarsi: R. Borruso, *Computer e diritto*, Tomo II, cit., p. 301; AA.VV., *Banche di dati e tutela della persona*, Padova, 1985, che raccoglie le relazioni e gli interventi al convegno tenutosi a Verona il 2 giugno 1984; AA.VV., *Le Banche dati in Italia*, Napoli, 1985, nel quale sono riportati in appendice le proposte ed avanzate per la disciplina della materia; AA.VV., *Banche dati, telematiche e tutela della persona*, Napoli, 1985; G. Mirabelli, *Osservazioni e rilievi allo schema del disegno di legge sulle banche di dati*, in *I Quad. giust.*, 1983, p. 27; Normando, *Iniziative di legge italiane per la regolamentazione delle banche di dati e per la tutela dei diritti alla personalità*, in *Crit. dir.*, 1984, p. 37; G. Alpa, *Raccolta di informazioni, protezione dei dati e controllo degli elaboratori elettronici (in margine ad un progetto di convenzione del Consiglio d'Europa)*, in *Foro it.*, 1982, mon., p. 27; S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1983; M. Petrone, *Banche dati e tutela della privacy. Riflessi penalistici*, in questa *Rivista*, 1988, p. 81; A. Traversi, *op. cit.*, p. 48; M.M. Correra, P. Martucci, *I reati connessi con l'uso del computer*, Milano, 1986.

di provvedere, almeno in parte, al contemperamento degli interessi conflittuali collegati all'esercizio delle banche di dati, ha sollecitato la presentazione di alcune proposte e disegni di legge. Dall'analisi dei relativi testi si possono ricavare indicazioni utili per l'argomento che interessa; particolarmente significativo è al fine il disegno di legge n. 1657 (Costituzione ed esercizio delle Banche di dati personali ad elaborazione informatica) presentato il 5 maggio 1984 dal Ministro di Grazia e Giustizia[49].

In primo luogo, si è ritenuto opportuno il ricorso alla sanzione penale, in funzione preventiva, rispetto ai danni tipici conseguenti al funzionamento delle banche dati. In secondo luogo, è stata avvertita la necessità di puntualizzare alcuni obblighi (ed i conseguenti effetti giuridici) su persone determinate, onde eludere il fenomeno dell'anonimia dei danni caratteristico delle complesse organizzazioni produttive. Si è in particolare prevista la figura del « Responsabile della banca dati » (art. 3) che deve essere nominato all'atto della costituzione della stessa. Il responsabile è destinatario di una serie di obblighi: provvedere alla notificazione all'autorità competente dell'esistenza della banca dati e del suo oggetto (art. 11); provvedere all'avviso agli interessati dell'avvenuta inserzione di dati che li riguardano (art. 13), reffificare o cancellare i dati inesatti, eccedenti, illegittimamente raccolti o carenti (art. 14, n. 3 e 4), inserire i dati su richiesta della persona che vi abbia interesse giustificato (art. 14, n. 5).

L'apparato sanzionatorio predisposto nel disegno di legge può anche apparire ipertrofico atteso che qualunque violazione degli obblighi determina l'insorgere della responsabilità penale. Le fattispecie previste possono distinguersi a seconda che prevedano un reato proprio del responsabile (è il caso dell'omessa cancellazione o rettifica sanzionata dall'art. 28) od un reato comune (si tratta delle fattispecie descritte dagli artt. 24, 25, 26 e 27) di cui possono rispondere anche soggetti non qualificati, ma che di regola dovrebbero finire col rivolgersi al responsabile, destinatario degli obblighi relativi alle violazioni stesse.

Si è al riguardo rilevato che « ove tali norme venissero approvate i soggetti che gestiscono una banca dati (usiamo questa espressione nella sua accezione più generica per indicare anche soggetti che si trovano al vertice di enti, associazioni o società che eventualmente gestiscono la banca dati) diverrebbero titolari di una posizione di garanzia per l'impedimento di reati che appaiano una specifica espressione dei pericoli insiti nell'attività esercitata »[50].

[49] Il testo del disegno di legge è riportato in Appendice al volume *Le Banche dati in Italia*, cit., p. 235 ss.

[50] G. GRASSO, *op. cit.*, p. 125.

5. Robotica e tutela penale del lavoro.

Nell'ambito dei sistemi esperti una peculiare problematica potrebbe porsi in merito all'applicazione della robotica nelle imprese ed ai pericoli eventualmente ad essa inerenti per la sicurezza del lavoro.

Come noto, il diritto positivo disciplina dettagliatamente (attraverso il d.P.R. 27 aprile 1955, n. 547 e il d.P.R. 19 marzo 1956, n. 302) le misure da apprestarsi per impedire gli infortuni sul lavoro; senonché nessuna di queste norme concerne specificamente la robotica (tecnologia non applicata quando veniva emanata la normativa antinfortunistica); pur non potendosi escludere che alcune delle norme preventive vigenti si rivelino valide ed efficaci anche in relazione a questi nuovi macchinari, risulterebbe, tuttavia, opportuno approfondire l'aspetto propriamente tecnico della questione, onde riscontrare quali incidenti possa determinare l'impiego della robotica nelle imprese e quali siano le misure idonee a prevenirli. I risultati di tale indagine potrebbero essere recepiti in una legislazione specifica, che introduca illeciti contravvenzionali. Intanto la determinazione dei meccanismi opportuni di salvaguardia è demandata alla sensibilità ed attenzione dei costruttori e degli imprenditori. Una funzione sanzionatoria indiretta può nel contempo rivestire la clausola generale dell'art. 2087 cod. civ. — in forza della quale « l'imprenditore è tenuto ad adottare nell'esercizio dell'attività d'impresa le misure che, secondo la particolarità del lavoro, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro » — che secondo la prevalente dottrina costituisce valido parametro, ai fini della valutazione della responsabilità per omissione dolosa di cautele contro infortuni sul lavoro (art. 437 cod. pen.) o per l'ipotesi colposa descritta dall'art. 451 cod. pen. Non si ritiene necessaria per la configurabilità di tali reati la specifica previsione della cautela o del dispositivo di prevenzione[51].

6. Responsabilità della gestione: modelli sanzionatori.

Questo primo tentativo di sintesi ha condotto ad una ricostruzione in senso frammentario e disorganico della responsabilità dei preposti alla gestione dei sistemi informatizzati. Si è confermata l'osservazione iniziale secondo cui dall'impossibilità di vedere nel sistema stesso un centro d'imputazione di effetti giuridici non poteva scaturire una correlativa ed automatica responsabilità del *management*,

[51] G. Fiandaca, E. Musco, *Diritto penale, parte spec.*, Bologna, 1988, p. 385 ss.; C. Smuraglia, *La sicurezza del lavoro e la sua tutela penale*, Milano, 1981, p. 159; T. Padovani, *Diritto penale del lavoro*, Milano, 1976, p. 160.

anche se attraverso i principi vigenti deve risalirsi da alcuni fatti al soggetto che li ha determinati attraverso il sistema stesso. Alla delicata natura ed alla quantità delle funzioni svolte dalle nuove strutture tecnologiche corrisponde un panorama lacunoso, quanto all'imputazione delle attività e delle conseguenze penalmente rilevanti: assenza di normativa specifica e difficoltà a risalire (sotto il profilo teorico e tecnico investigativo) alla fonte umana di un inadeguato funzionamento del sistema. Deve però rilevarsi che l'attuale situazione è in parte giustificata dai principi di tipicità e di personalità dell'illecito che caratterizzano il sistema penale.

Ciò posto queste lacune non possono essere che in minima parte superate attraverso l'istituzione di un « responsabile » del sistema, costruendo una figura parallela ed analoga a quella richiesta per i sistemi — banche dati. Va, infatti, ribadito che il responsabile non può divenire un centro automatico d'imputazione di tutte le conseguenze dell'attività del sistema od un mezzo di canalizzazione degli eventuali rischi che si ritenessero connessi all'attività informatizzata. Non si potrebbe in particolare creare, senza snaturarne il fondamento, una fattispecie analoga a quella introdotta in materia di stampa dall'art. 57 cod. pen.[52]: basti considerare che al Direttore responsabile compete un controllo di natura preventiva sulla liceità della pubblicazione; controllo che, per quanto sia sempre più arduo da realizzare, resta concretamente attuabile. Ciò rende possibile ricondurre sotto il dominio del Direttore responsabile il contenuto della pubblicazione e sanzionare l'omesso controllo correlato ad un illecito penale di terzi. Il Responsabile del sistema si troverebbe, per contro, nella concreta impossibilità di prevenire la commissione di reati, esorbitando dal suo controllo diretto la globale attività della struttura (in considerazione della massa dei dati trattati) e versando egli nell'incapacità tecnica — almeno nella maggior parte dei casi — di esercitare un sindacato sull'efficienza del programma prima che questo abbia manifestato tangibilmente i suoi vizi. Essendo inesigibile l'obbligo di garantire il carattere lecito dell'attività del sistema gestito, una fattispecie coniata sulla falsariga dell'art. 57 cod. pen. non potrebbe essere introdotta in relazione ai sistemi informatizzati, senza violare i principi di natura costituzionale e principalmente l'art. 27 Cost. e senza rilevarsi inopportuna perché, riducendosi ad

[52] L'inquadramento della fattispecie di cui all'art. 57 cod. pen. — che ha dato luogo a perplessità e polemiche — resta controverso anche dopo l'intervento legislativo: propende per qualificarla come ipotesi di responsabilità obiettiva: G.D. PISAPIA, *La nuova disciplina per i reati commessi a mezzo della stampa*, in *Riv. it. dir. proc. pen.*, 1958, 321. Ritengono si tratti di un'ipotesi di responsabilità colposa: F. ANTOLISEI, *Manuale, parte gener.*, cit., p. 342; G. FIANDACA, E. MUSCO, *Diritto penale, parte gener.*, cit., p. 361; G. DELITALIA, *Titolo e struttura della responsabilità penale del direttore del giornale per i reati commessi a mezzo della stampa periodica*, in *Riv. it. dir. proc. pen.*, 1959, p. 556; F. MANTOVANI, *Dir. pen.*, cit., p. 373; C.F. GROSSO, *Responsabilità penale per i reati commessi col mezzo della stampa*, Milano, 1969, p. 87; P. NUVOLONE, *Il sistema del diritto penale*, Milano, 1982, p. 368; A. PAGLIARO, *op. cit.*, p. 353.

una forma di responsabilità per il mero *status* del soggetto, non svolgerebbe alcuna concreta funzione di prevenzione. Superfluo rilevare che per i medesimi principi e per le medesime esigenze non potrebbe imputarsi automaticamente al responsabile — a prescindere cioè dalla valutazione dell'efficienza condizionante della condotta e della sussistenza della colpa — gli eventi penalmente rilevanti determinati da un erroneo funzionamento del sistema.

Se si dovesse rilevare la necessità di potenziare gli strumenti sanzionatori, potrebbe legittimamente imporsi ad un « Responsabile » di adottare le misure precauzionali che dovessero mostrarsi necessarie a ridurre o controllare un eventuale rischio che si manifestasse intrinsecamente presente nell'attività informatizzata, od anche in relazione a talune delle attività informatizzate. Per ottenere il soddisfacimento delle esigenze precauzionali, potrebbero idearsi figure di illecito, anche a contenuto omissivo. Conformemente ai più recenti orientamenti emersi in tema di politica criminale e di tecniche di tutela, si rileverebbe però l'opportunità di ricorrere alla sola sanzione amministrativa, per la repressione di quelle condotte meramente disobbedienti non ancora produttive di un effettivo pericolo per il bene protetto, considerato anche che tale forma di illecito si rileva di più agevole ed efficace applicazione nei confronti di strutture organizzative complesse[53]. Rispetto a talune ipotesi, da individuarsi attentamente e partitamente, potrebbero peraltro introdursi singole fattispecie di agevolazione colposa, ritenute efficaci rispetto a « fatti penalmente rilevanti nell'ambito di enti dotati di struttura organizzativa complessa », per « sottolineare quei doveri di controllo nei confronti di attività illecite dei propri sottoposti, che di regola possono sorgere a carico dei soggetti dotati di responsabilità direttive »[54].

Il ricorso a sanzioni penali si può profilare, in questo settore, opportuno, atteso che la risposta civilistica si è rilevata insufficiente: è stato infatti, considerato che « proprio in campo tecnologico, la responsabilità oggettiva non svolge un'adeguata funzione deterrente, perché le passività rappresentate dal costo del risarcimento dei danni collegati comunque al funzionamento delle attività tecnologiche è ampiamente assorbita e compensata dal margine di profitto che proprio le tecnologie più rischiose consentono a chi le utilizza »[55].

[53] A. CADOPPI, *Il reato omissivo proprio*, vol. I, Padova, 1988, p. 370, ed, in generale, F. BRICOLA, *Tecniche di tutela penale e tecniche alternative di tutela*, in *Funzioni e limiti nel diritto penale. Alternative di tutela*, p. 60.

[54] F. ALBEGGIANI, *op. cit.*, p. 226; A. CADOPPI, *op. loc. cit.*