DÉSIRÉE FONDAROLI

LA TUTELA PENALE DEI « BENI INFORMATICI »

SOMMARIO: 1. Premessa: interrogativi circa la necessità di una normativa *ad hoc*. — 2. L'estensione della disciplina del diritto d'autore ai programmi per elaboratore (d.lgs. 29 dicembre 1992, n. 518). — 3. I principi della legge n. 547 del 1993. — 4. La tutela del patrimonio informatico. — 5. (*segue*) La truffa informatica. — 6. La tutela della riservatezza: una lacuna legislativa prossima ad essere colmata. — 7. (*segue*) *a*) l'accesso abusivo ad un sistema informatico o telematico. — 8. (*segue*) *b*) le interpolazioni nelle comunicazioni informatiche o telematiche. — 9. Il concetto di « documento informatico » e le relative ipotesi di falsità. — 10. Il diritto penale delle carte di credito.

1. PREMESSA: INTERROGATIVI CIRCA LA NECESSITÀ DI UNA NORMATIVA *AD HOC*.

Il d.lgs. 29 dicembre 1992, n. 518 e la legge 23 dicembre 1993, n. 547 disciplinano alcuni fenomeni attinenti alla c.d. criminalità informatica, nel tentativo di allineare l'ordinamento italiano alle disposizioni della Unione Europea e alle legislazioni dei Paesi che ad essa appartengono.

Decisiva in tal senso è l'esigenza della cooperazione internazionale, condizionata dal principio della « doppia incriminazione ». Come sottolinea la Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice Penale in tema di criminalità informatica, poi trasfuso nella legge vigente[1], l'ordinamento che non abbia previsto fattispecie incriminatrici in materia dovrebbe negare la propria cooperazione agli Stati richiedenti.

L'intervento espresso e settoriale del legislatore si è reso necessario per la lacunosità della normativa previgente, che concerneva « fatti illeciti » ben lontani, sia dal punto di vista della individuazione del bene giuridico protetto, sia sotto il profilo della condotta e dell'oggetto « materiale » del reato, dai c.d. *computers crimes* generati dall'evoluzione della tecnologia informatica[2].

[1] Cfr. in *Documenti Giustizia*, 1991, 145.

[2] Le perplessità in materia sono tali e tante, che non si è giunti nemmeno ad una comune « denominazione » del fenomeno: se nell'ordinamento francese si definisce in generale il fenomeno quale *fraude informatique*, l'ordinamento tedesco conosce la *Computerkriminalität*, mentre nei Paesi anglosassoni si è fatto riferimento prima alla « criminalità da *computer* », poi ai *computer crimes*: sul punto cfr. an-

Si tratta di arginare un fenomeno di estensione più ampia di quanto si possa immaginare, poiché non solo minaccia la sfera della vita privata e del patrimonio, ma consente la rapidissima circolazione delle informazioni, venendo così a costituire un efficace « mezzo di comunicazione », largamente utilizzato dalle associazioni illecite sia, ad esempio, come veicolo di diffusione di propaganda terroristica o antirazzista, sia come « *nuova frontiera* » della criminalità organizzata[3].

La prima questione posta sul tappeto concerne l'opportunità o meno di assoggettare a sanzione penale le condotte di interferenza nel sistema di elaborazione informatica.

Criterio guida al riguardo dovrebbe rimanere, infatti, il principio della natura di *extrema ratio* del diritto penale[4]. In essa trova radici la tesi che àncora la tutela penale a beni giuridici « consolidati »[5]. Tuttavia gli ordinamenti europei, sordi a tale insegnamento — ciò a differenza dei sistemi angloamericani che fanno un uso prudente della disciplina penale in materia di « illeciti informatici » — sembrano ricorrere volentieri allo strumento penale, soprattutto in considerazione della sua funzione « stigmatizzante » e « simbolica ».

La questione va affrontata nella prospettiva ben evidenziata da un recente scritto di Giovanni Fiandaca e di Enzo Musco[6]: la necessità dell'intervento penale nasce dal difficile equilibrio tra riflessione dottrinale e « percezione sociale » del ruolo del diritto penale stesso nella società.

Negare quest'ultimo profilo per arroccarsi acriticamente nella « torre d'avorio » della strenua difesa del principio del diritto penale quale *extrema ratio* ostacola la ricerca per la soluzione del problema.

Se si prescinde dalle ipotesi in cui il sistema di elaborazione dei dati è mero strumento attraverso il quale si pone in essere la condotta criminosa, può osservarsi che gran parte delle difficoltà in merito alla punibilità dei « fatti » di c.d. criminalità informatica risiede nella peculiarità della « informazione », che rappresenta l'elemento caratterizzante la trasmissione telematica ed, in ultima analisi, l'oggetto « materiale » della condotta illecita.

L'« informazione », in quanto tale, evidenzia sempre e comunque un problema di tutela della riservatezza.

Che, in particolare, a garanzia della inviolabilità della riservatezza lo strumento di intervento statale debba essere necessariamente quello penale, è opzione da ponderare attentamente: le considerazioni, in questa sede, non possono che essere sintetiche.

Un passo significativo nella direzione del riconoscimento della « riservatezza » come autonomo bene giuridico meritevole di tutela penale è com-

---

che L. Picotti, *Studi di diritto penale dell'informatica*, Verona, 1992, 12 ss.

[3] V. Militello, *Informatica e criminalità organizzata*, in *Riv. trim. dir. pen. econ.*, 1990, 81 ss. Sulle applicazioni illecite delle più moderne tecnologie informatiche si veda anche U. Sieber, *Computerkriminalität und Informationsstrafrecht*, in *Computer und Recht*, 1995, 105.

[4] F. Bricola, voce *Teoria generale del reato*, in *Noviss. Dig. it.*, 1973, 7 ss.; Id., *Tecniche di tutela penale e tecniche alternative di tutela*, in Aa.Vv., *Funzioni e limiti del diritto penale*, Padova, 1984, 3 ss.; W. Hassemer, *Kennzeichen und Krisen des modernen Strafrechts*, in *ZRP*, 1992, 383.

[5] In tale ultimo senso cfr. A. Rossi Vannini, *La criminalità informatica: le tipologie di* computer crimes *di cui alla legge n. 547/1993 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. dir. pen. econ.*, 1994, 433.

[6] G. Fiandaca - E. Musco, *Perdita di legittimazione del diritto penale?*, in *Riv. it. dir. proc. pen.*, 1994, 25 ss.

piuto dal Progetto di legge delega che al titolo VI del Libro I contempla appunto la disciplina dei reati contro la riservatezza[7]. Il riconoscimento a livello normativo della tutela penale della *privacy* rappresenterebbe un fattore decisivo anche nella prospettiva di una più ampia riflessione sui « beni » della personalità. In tale contesto ben si comprende la rilevanza della direttiva europea 95/46/CE (sulla quale torneremo in seguito) il cui art. 1 garantisce (in particolare) la tutela alla vita privata, con riguardo al trattamento dei dati personali[8].

Qualche isolata scintilla di tale tutela sembra essere già presente nell'ordinamento vigente[9]. Nella legge 7 agosto 1990, n. 241, che disciplina il diritto di accesso agli atti amministrativi, l'art. 24, comma 2, lett. *d*), garantisce « la riservatezza di terzi, persone, gruppi o imprese ». Sintomatica in tal senso appare una recente decisione del Consiglio di Stato[10] che, in relazione alla problematica della trasparenza degli atti amministrativi (legge 7 agosto 1990, n. 241), ha affermato la preclusione dell'accesso agli atti amministrativi, qualora venga leso il diritto alla riservatezza: « mentre il diritto alla riservatezza, quale diritto della personalità, afferendo direttamente alla salvaguardia del complesso delle situazioni attraverso le quali si realizza la sfera privata, assume una connotazione di immediato rilievo sostanziale, ''la cura e la difesa degli interessi giuridici'', cui fanno riferimento le disposizioni sopra dette[11], avendo riguardo ad una posizione giuridica strumentale, deve evidentemente essere specificata in relazione al contenuto precipuo dell'interesse da curare e difendere, potenzialmente idoneo a delimitare l'ambito di operatività del diritto alla riservatezza ».

Ma, naturalmente, la questione travalica la circoscritta tematica della protezione della riservatezza per investire il tradizionale dibattito intorno al bene giuridico ed in particolare, come si è anticipato, all'opportunità di assegnare al « patrimonio informatico » o alla « informazione » *lato sensu* dignità di bene giuridico penalmente protetto[12].

---

[7] Cfr. in *Documenti Giustizia*, 1992, 3, 421. Sul punto cfr. anche *infra* nel testo par. 6.

[8] A. Manna, *Tutela penale della personalità*, Bologna, 1993, 96 ss.; Id., *Beni della personalità e limiti della protezione penale*, Milano, 1989, 3 ss. e 260 ss.

[9] Significativo, in tema di riconoscimento di « diritto alla riservatezza », l'art. 8, comma 1, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, e resa esecutiva in Italia con legge 4 agosto 1955, n. 848 (per una interessante applicazione di tale norma cfr. Cass. civ. 27 maggio 1975, n. 2129, in *Riv. dir. int.*, 1980, 293 ss.). Oltre alla Convenzione di Strasburgo sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale adottata il 28 gennaio 1981 e ratificata dallo Stato italiano con legge 21 febbraio 1989, n. 98, la normativa penale a tutela della riservatezza appare frammentaria: si vedano le disposizioni citate *infra* in nota 59; cfr. L. Sola, *I computer crimes nell'ordinamento giuridico italiano: alcune considerazioni*, in L. Sola - D. Fondaroli, *A proposito della criminalità informatica*, Bologna (Clueb), 1992, 18 ss.

[10] Cons. Stato, Sez. VI, 20 maggio 1994-10 gennaio 1995, n. 13, in *Guida normativa*, 1995, n. 25, 21 ss.

[11] Ovvero gli artt. 24, comma 2, lett. *d*), legge n. 241/1990 e 8, comma 5, legg. *d*), d.P.R. 27 giugno 1992, n. 352.

[12] Sulla funzione e sui limiti del concetto di bene giuridico la bibliografia è sterminata. Per alcuni spunti di riflessione si vedano Amelung, *Rechtsgüterschutz und Schutz der Gesellschaft*, 1972, 15; M. Marx, *Zur Definition des Begriffs « Rechtsgut »*, 1972, 4; Hassemer, *Il bene giuridico nel rapporto di tensione tra Costituzione e diritto naturale*, in *Dei delitti e delle pene*, 1984, 274; Stella, *La teoria del bene giuridico e i c.d. fatti inoffensivi conformi al tipo*, in *Riv. it. dir. proc. pen.*, 1973, 3; E. Musco, *Bene giuridico e tutela dell'onore*, 1974, 55; F. Angioni, *Contenuto e funzioni del concetto di bene giuridico*, 1983, 14; G. Fiandaca, *Il « bene giuridi-*

A fronte del principio di necessario ancoraggio — anche solo implicito — dei beni penalmente protetti al dettato costituzionale[13], vi è una tendenza volta ad accogliere tesi incentrate sulla opportunità di determinare la tutelabilità penale dei beni giuridici alla stregua delle esigenze palesate dai conflitti in essere nel conteso sociale[14].

La discussione porterebbe il discorso lontano dagli angusti confini di questa ricerca.

Ciò che preme sottolineare — e che non vuole certo assumere i toni di una « scoperta », ma soltanto la conferma della lucidità di considerazioni già note — è che la concezione e la rilevanza del bene giuridico nella moderna dommatica devono fare i conti con due tendenze talvolta conflittuali: da un lato, l'affermarsi di principi ed elaborazioni mirate alla rinuncia o quanto meno alla sospensione della esecuzione della pena; dall'altro, il « reclutamento » nell'ambito del diritto penale di illeciti fino ad ora rimasti estranei al tessuto normativo penale, con conseguente predominanza dell'area delle lesioni di beni giuridici collettivi (universali) rispetto a quelli individuali[15].

Nella discussione sulla assoggettabilità a pena dell'illecito informatico le istanze di rassicurazione della società hanno prevalso[16]: la prescelta via della sanzione penale, tuttavia, si è dimostrata difficile da percorrere, quanto meno sotto due profili.

Innanzi tutto l'individuazione delle condotte punibili non avviene *de plano*, posto che l'elaboratore informatico, nonché i dati ed i programmi, appaiono di volta in volta come « oggetto » materiale del reato, « strumento » attraverso il quale il reato è posto in essere, « oggetto agente » del reato stesso[17].

Né le difficoltà si arrestano a questo punto.

Enucleati i potenziali « fatti » criminosi, si tratta poi di identificare le disposizioni astrattamente applicabili, e di verificarne la concreta operatività.

Quanto alla delimitazione dei « fatti » suscettibili di incriminazione, la dottrina in materia, confortata dalla Risoluzione del Consiglio d'Europa, si è concordemente espressa nel senso di circoscrivere la scelta ad alcune ipotesi di base: accesso e uso non autorizzato dell'elaboratore; danneggiamento di dati, *software* e *hardware*; falsità di dati e/o programmi; interfe-

---

co » come problema teorico e come criterio di politica criminale, in AA.VV., *Bene giuridico e riforma della parte speciale*, a cura di A.M. STILE, Napoli, 1985, 3 ss.; F.ANGIONI, *Beni costituzionali e criteri orientativi sull'area dell'illecito penale*, in AA.VV., *Bene giuridico e riforma della parte speciale*, cit., 57 ss.; e, di recente, A. MANNA, *Tutela penale della personalità*, cit., 20 ss.

[13] Per citare soltanto alcuni Autori cfr. F. BRICOLA, voce *Teoria generale del reato*, cit., 14; ID., *Tecniche di tutela penale e tecniche alternative di tutela*, in AA.VV., *Funzioni e limiti del diritto penale*, a cura di DE ACUTIS - PALOMBARINI, Padova, 1984, 7; G. FIANDACA, *Il « bene giuridico » come problema teorico e come criterio di politica criminale*, in *Riv. dir. pen. proc. pen.*, 1982, 52.

[14] In tal senso tra gli altri cfr. E. DOLCINI - G. MARINUCCI, *Costituzione e politica dei beni giuridici*, in *Riv. it. dir. proc. pen.*, 1994, 349; PAGLIARO, *Principi di diritto penale. Parte generale*, Milano, 4ª ed., 1993, 226.

[15] W. HASSEMER, *Spunti per una riflessione sul tema « bene giuridico e riforma della parte speciale »*, in AA.VV., *Bene giuridico e riforma della parte speciale*, cit., 367.

[16] G. CARLESI, *La criminalità informatica*, in *Informatica ed enti locali*, 1988, 501 ss.; U. SIEBER, *Computerskriminalität*, cit., 107.

[17] D.B. PARKER, *Crime by Computer*, New York, 1976, 12.

[18] Circa i limiti di tale « elenco mini-

renze illecite nel programma; frode (anche attraverso il « servizio Bancomat »); riproduzione non autorizzata di programmi per elaboratore[18].

Controversa invece l'opportunità di sanzionare penalmente il c.d. furto di dati informatici, che, come si vedrà, presuppone l'ammissibilità di una sorta di furto di informazione. Non diversa, sotto questo profilo, la problematica circa la configurabilità delle ipotesi di danneggiamento informatico, risolte poi dalla legge n. 547/1993.

Oggetto « materiale », ovvero oggetto su cui incidono le condotte criminose, sono i dati ed i programmi per elaboratore. In particolare, la natura dei beni in questione, cioè la loro essenza di beni « immateriali », determina non poche difficoltà.

Non che, come si è acutamente messo in luce[19], la tutela dei beni « immateriali » sia del tutto estranea al sistema sanzionatorio vigente.

Tuttavia è evidente che l'universo della elaborazione informatica manifesta natura e caratteristiche diverse dai tradizionali « oggetti materiali » del reato conosciuti dall'ordinamento penale italiano, ivi comprese le cc.dd. opere dell'ingegno, ed appare refrattario a farsi imbrigliare nelle maglie delle rigide definizioni normative.

Infatti, precedentemente alla entrata in vigore delle citate riforme del 1992 e del 1993, la normativa contenuta nel Codice Rocco e nella disciplina del diritto di autore (legge 22 aprile 1941, n. 633) — quest'ultima chiamata in causa per tutelare il *software*, in via di interpretazione estensiva, quale opera dell'ingegno — non presentava problemi di operatività quando le condotte criminose avessero ad oggetto la « macchina », l'elaboratore in senso tecnico. In tali casi la condotta criminosa insiste su un oggetto materiale (l'elaboratore, appunto), i cui requisiti di « materialità » e « fisicità » sono compatibili con la descrizione contenuta nel testo normativo. Così, non hanno posto problemi applicativi le condotte di danneggiamento o il furto del *computer* inteso come struttura meccanica, né comportamenti aventi ad oggetto i supporti materiali (ad esempio, i *floppy*) su cui siano memorizzati i programmi o i dati.

Le maggiori difficoltà, invece, si sono riscontrate laddove le condotte criminose abbiano aggredito direttamente beni « immateriali » quali il *software* o i dati informatici.

In tali ipotesi viene meno il dato della « materialità » su cui si incentrano, ad esempio, le fattispecie incriminatrici tipiche di furto, appropriazione indebita, danneggiamento e truffa. Riguardo a queste il dato normativo è palese: oggetto « materiale » della condotta è la « cosa mobile ». A detto concetto non appare facilmente riconducibile l'informazione contenuta nel dato immagazzinato nel *computer* né il dato o il programma in se stesso.

Il bene immateriale non può quindi appartenere al concetto di « cosa mobile » sottesa dalle norme del Codice Penale.

Una applicazione della normativa vigente alle ipotesi di c.d. criminalità informatica significherebbe quindi una palese violazione dell'art. 25 della Costituzione sotto il profilo del divieto di analogia *in malam partem*. In

---

mo » di reati da prevedere in materia cfr. la Raccomandazione n. R (89) 9 del Comitato dei Ministri ai Paesi membri sulla criminalità connessa agli elaboratori elettronici, in *Riv. it. dir. pen. econ.*, 1992, I, 378. Sul punto si tornerà in seguito.

[19] L. Picotti, *Studio di diritto penale dell'informatica*, cit., 5 ss.

tali termini si è espresso l'orientamento prevalente[20], sebbene non siano mancati isolati riconoscimenti della operatività della fattispecie in omaggio ad una interpretazione (ritenuta) estensiva (e non quindi analogica) delle fattispecie stesse[21].

I casi pratici offerti all'esame della giurisprudenza presentano poi altre peculiari caratteristiche.

Non ha riscontro, ad esempio, la tesi favorevole alla applicazione, nei casi di specie, della disciplina relativa al furto.

A voler prescindere dalla circostanza che oggetto di furto deve pur sempre essere una « cosa mobile », va osservato che le condotte assimilabili al furto sono caratterizzate per lo più dalla duplicazione di programmi. La condotta, tuttavia, raramente implica lo « spossessamento » dei dati o del programma (nei confronti del legittimo titolare di essi) e, per converso, l'« impossessamento » da parte dell'agente. Eppure impossessamento e spossessamento del bene materiale connotano proprio il delitto di furto.

Nel caso dei dati e dei programmi, invece, questi restano nella memoria dell'elaboratore, ma la informazione che essi contengono viene riprodotta e trasmessa o, comunque, divulgata. È l'informazione, quindi, a dover essere « rubata », perché possa legittimamente parlarsi di furto.

A fronte della tesi della applicazione del delitto di furto, nel caso di duplicazione del programma, si è anche sostenuto che le azioni di appropriazione o « impossessamento » e di « spossessamento » hanno diversa natura a seconda del bene materiale su cui incidono, con la conseguenza che il bene « materiale » (come un qualsiasi elemento appartenente al mondo fenomenico) presuppone necessariamente una « captazione » di tipo materiale, mentre il bene « immateriale », quale appunto l'informazione, può essere oggetto di una forma di apprensione di tipo immate-

---

[20] L. PICOTTI, *La rilevanza penale degli atti di sabotaggio*, in questa *Rivista*, 1986, 505; GRECO, *Osservazioni in materia di attentato a impianti di pubblica utilità*, in *Giur. mer.*, 1988, II, 392; Trib. Torino, uff. istr., 12 dicembre 1983, in *Giur. it.*, 1984, II, 352 ss. (ove si esclude tanto l'ipotesi del furto quanto quella del danneggiamento per la mancanza dei requisiti di specie, senza tuttavia entrare nel merito della questione della applicabilità delle disposizioni ai beni mobili o immobili). Notiamo che il materiale giurisprudenziale in tema di criminalità informatica appare limitato (il fenomeno naturalmente non è soltanto italiano, investendo la natura stessa della tipologia del reato in esame: cfr. D. ZIELINSKI, *Anmerkung BGH 10 novembre 1994*, in *NStZ*, 1995, 345): difficilmente infatti le ipotesi criminose in questione vengono rese note ai Tribunali a causa dei problemi di « immagine » e « serietà » che dalla divulgazione di notizie relativi alla vulnerabilità dei sistemi informatici possono scaturire per gli operatori economici, al cui novero appartiene la maggior parte delle « vittime » della criminalità informatica. Le medesime questioni sono state affrontate riguardo alla applicazione al software dell'art. 171 l. n. 633/41 relativa ala tutela del diritto d'autore: cfr. *infra*, nota ([24]).

[21] Nel senso della applicabilità della normativa in tema di truffa (art. 640 cod. pen.) cfr. Trib. Roma 20 giugno 1985, in questa *Rivista*, 1986, 166. L'operatività della norma sul danneggiamento (art. 635 cod. pen.) è stata ammessa facendo leva sul concetto di « sistema informatico », nel quale la distinzione tra *software* (bene immateriale) ed *hardware* (struttura materiale) viene a scomparire: « le modifiche di un programma possono essere considerate sia come alterazioni materiali che come cambiamenti strutturali alla prestazione di un sistema, in quanto ne compromettono la funzionalità, lo rendono inservibile all'uso cui è destinato » (Trib. Torino 23 ottobre 1989, in *Foro it.*, 1990, II, 468). Analogamente, sebbene in modo meno elaborato, si era deciso circa l'operatività dell'art. 420 cod. pen. in una ipotesi di presunto « sabotaggio »: cfr. Trib. Firenze, uff. istr., 27 gennaio 1987, in *Foro it.*, 1986, II, 359.

riale[22]. In tale ottica anche il furto di informazione non apparirebbe così paradossale come potrebbe desumersi da in prima battuta.

Tuttavia una tesi siffatta, per quanto sensibile ad una visione in chiave dinamica del dettato normativo, collide con una osservazione di fondo: ovvero con la tassatività del disposto legislativo, che circoscrive l'ambito di applicazione della norma vigente alla « cosa mobile ». In omaggio al principio di determinatezza e riserva di legge, pertanto, la incriminazione di un fatto non può che discendere da una espressa previsione legislativa. Se dunque opportuno pare assoggettare a sanzione tale comportamento, necessaria diviene la modificazione o l'integrazione della disposizione, perché fattispecie come il furto informatico trovino cittadinanza nell'ordinamento penale italiano.

Osserviamo fin da ora, per riprendere poi l'argomento oltre, che l'esito della ricognizione delle norme codicistiche previgenti alla legge n. 547/1993 appare deludente.

Il secondo passo sulla via del riconoscimento di una qualche forma di tutela autonoma del programma o del dato informatico si è percorso prendendo in esame la tutela del diritto d'autore (artt. 1, 2 e 171, legge n. 633/1941). In tal caso, infatti, la riproduzione di dati o programmi sembra integrare la violazione della proprietà « intellettuale », che è protetta quale « bene immateriale ».

La questione si è posta — e continua tuttora a rappresentare una delle ipotesi di violazione più frequentemente sottoposte alla attenzione della magistratura — in relazione alla duplicazione dei programmi per videogiochi.

La disciplina rilevante a riguardo è la citata legge n. 633/1941, il cui art. 171 stabilisce le sanzioni per le ipotesi di duplicazione e diffusione abusiva dell'opera dell'ingegno.

Presupposto della operatività della norma è la qualificazione del *software* come opera dell'ingegno, caratterizzata dalla creatività ed originalità, e riconducibile all'elenco previsto dagli artt. 1 e 2, legge n. 633/1941, che nella versione antecedente alla riforma del 1992 non conteneva alcun riferimento al programma per elaboratore.

La giurisprudenza civile, svincolata dal rispetto del principio costituzionale del divieto di analogia *in malam partem*, nonostante il silenzio legislativo non ha avuto dubbi nel qualificare il *software* come opera dell'ingegno. A sostegno della tesi si è addotta l'originalità della forma espressiva e dello stile del *software*, testimonianza dello sforzo creativo dell'autore. Il programma per elaboratore è stato pertanto considerato come opera scientifica (ai sensi dell'art. 2, legge n. 633/1941), da annoverare tra le opere della letteratura *ex* art. 1, l.d.a.[23].

Di diverso avviso sul punto la prevalente giurisprudenza penale di merito che ha sottolineato, oltre al divieto di analogia *in malam partem*, anche l'incompatibilità strutturale tra il programma per elaboratore e quella particolare opera dell'ingegno che è l'opera letteraria, cui esso potrebbe essere assimilato per il suo contenuto di raccolta e trasmissione di informazioni[24].

---

[22] M.P. Lucas de Leyssac, *Il furto d'informazione*, in questa *Rivista*, 1985, 625.

[23] Per tutti cfr. Pret. Roma 4 luglio 1988, Soc. IBM Italia c. Soc. BIT Computers ed altri, in *Foro it.*, 1988, I, 3132.

[24] Sintomatica in proposito Pret. Bologna 24 aprile 1986, in *Foro it.*, 1986, II, 515; Trib. Monza 26 luglio 1985, *ivi*, 519; Pret. Napoli, 6 giugno 1985, in *Riv. dir. ind.*, 1986, II, 69.

Al riconoscimento della tutela penale del *software* attraverso il diritto d'autore è comunque pervenuta la Corte di Cassazione, la quale ha riconosciuto nel programma per elaboratore (applicativo) il « prodotto di uno sforzo particolare di un intelletto specificamente educato e, soprattutto, votato alla scienza informatica », in quanto tale meritevole di tutela ai sensi della legge sul diritto d'autore[25].

L'avallo della Suprema Corte appare significativo, ma non sufficiente: permane l'ombra della discrezionalità della magistratura nella assimilazione della duplicazione e/o diffusione del programma per elaboratore a quella delle opere dell'ingegno. E sempre va ricordato che l'ordinamento italiano non riconosce efficacia vincolante al precedente giudiziario.

In questo panorama di incertezza l'intervento del legislatore è stato invocato da più parti, anche in considerazione dell'evoluzione legislativa dei Paesi europei[26] e della stessa (allora Comunità, oggi) Unione europea[27].

Ancora. L'allarme sociale generato dalla diffusività del fenomeno in esame sollecita soluzioni rapide, sebbene non necessariamente siano da ricercare nell'ambito di un intervento di tipo penale. Si calcola che nella sola Repubblica federale tedesca il mercato delle copie illecite dei programmi raggiunga il 76% degli esemplari in circolazione[28].

2. L'estensione della disciplina del diritto d'autore ai programmi per elaboratore (d.lgs. 29 dicembre 1992, n. 518).

Soltanto nel 1992 l'Italia risponde agli « imperativi » della Unione europea che estendono al programma per elaboratore la tutela del diritto d'autore[29].

---

[25] Cass. pen., Sez. III, 6 luglio 1987, in questa *Rivista*, 1987, 696: tra i presupposti a monte della decisione della Corte è l'affermazione della non tassatività delle classificazioni contenute nella disciplina. Con argomentazioni diverse ma pur nel senso della applicazione della norma penale nel caso di duplicazione illecita del programma informatico cfr. Pret. Napoli 7 giugno 1985, in *Riv. dir. ind.*, 1986, II, 69 s.

[26] Alcuni ordinamenti europei avevano già provveduto ad equiparare il programma per elaboratore all'opera dell'ingegno. Si pensi alla legge tedesca del 24 giugno 1985 (*Gesetz zur Änderung von Vorschriften auf dem Gebiet des Urheberrechts*), analizzata con particolare attenzione da L. Picotti, *Studi di diritto penale dell'informatica*, cit., 33 e 79 ss.; alla legge francese n. 85/660 del 3 luglio 1985, le cui norme sono state recepite dalla legge n. 92-597 del 1º luglio 1992, relativa al codice della proprietà intellettuale — artt. 1, 5, 112-1 e 111-2, da 335-2 a 335-4 (cfr. M. Mantovani, *I reati informatici nella recente esperienza francese: l'uso e l'accesso abusivi*, in questa *Rivista*, 1990, 885 ss. e D. Fondaroli, *I problemi della criminalità informatica e la legge francese n. 88-19 del 5 gennaio 1988*, in *Ind. pen.*, 1989, 762); infine, alla legge spagnola n. 22/1987 dell'11 novembre 1987.

[27] Direttiva n. 91/250/CEE del 14 maggio 1991.

[28] U. Sieber, *Computerkriminalität*, cit., 104.

[29] La direttiva prevedeva come termine ultimo per il recepimento il 1º gennaio 1993; il d.lgs. n. 518/1992 viene promulgato appena in tempo (29 dicembre 1992) per evitare allo Stato italiano di incorrere nella sanzione indiretta della applicazione « *self-executing* » delle direttive dettagliate e non recepite dagli Stati membri entro il termine previsto dalla direttiva stessa. Si tratta di uno spunto di riflessione interessante, che presuppone la prevalenza del diritto comunitario rispetto al diritto interno: in tale contesto, secondo l'orientamento dominante della Corte di Giustizia, il mancato o il tardivo recepimento della direttiva consente al cittadino del singolo Stato di adeguarsi direttamente alle disposizioni contenute nella direttiva comunita-

Significativa la direttiva europea n. 91/250/CEE, il cui art. 1.1[30] precisa che i programmi per elaboratore sono tutelati « come opere letterarie, non nel senso che essi siano *assimilabili* a queste ultime, ma nel senso che i programmi per elaboratori *hanno natura* di opere letterarie » (così anche la Relazione alla Direttiva, in corrispondenza del par. « Singole disposizioni », par. 1.2).

La mera qualificazione del programma per elaboratore (*software*) come opera dell'ingegno non appare determinante, per quanto necessaria per garantire almeno la tutela del diritto d'autore: la normativa europea prevede altresì una serie di disposizioni che consentono di armonizzare la tutela del diritto d'autore con la struttura di tali particolari beni.

Vero è che la direttiva opta per la tutela garantita al diritto di autore; essa, tuttavia non esclude l'applicazione di altre forme di tutela, rimesse alla discrezione dei singoli Stati (art. 9). Il legislatore italiano, ad esempio, si è avvalso di tale facoltà introducendo una normativa sulla tutela giuridica delle topografie dei prodotti a semiconduttori[31] (legge 21 febbraio 1990, n. 70).

Uniformandosi alle disposizioni della Direttiva, quindi, il d.lgs. n. 518/1992[32] contiene una integrazione degli artt. 1 e 2 della legge n. 633/1941, rispettivamente laddove al programma per elaboratore viene accordata protezione come opera letteraria ai sensi della Convenzione di Berna ratificata e resa esecutiva con legge 20 giugno 1978 (art. 1, d.lgs. n. 518/1992), con relativa inclusione del programma stesso tra le opere dell'ingegno elencate nell'art. 2 della stessa l.d.a. (art. 2, d.lgs. n. 518/1992).

Con l'art. 10, d.lgs. n. 518/1992, si è poi riscritta la disciplina sanzionatoria relativa al diritto d'autore, introducendo nella legge n. 633/1941 l'art. 171-*bis*, che diviene fattispecie assorbente. Infatti, la fattispecie *ex* art. 171 resta sussidiaria, come attesta la presenza dell'inciso « salvo

---

ria, o di chiedere al giudice l'applicazione di questa, anche in difformità o in contrasto con la normativa interna. Nel caso di specie, quindi, anche in assenza di una norma interna contenente la tutela del programma per elaboratore ad opere della legge sul diritto di autore, questa avrebbe comunque dovuto essere applicata secondo il dettato della direttiva n. 91/250. Sulla operatività *self-executing* delle direttive dettagliate e non recepite cfr. F. SGUBBI, voce *Diritto penale comunitario*, in *Dig. disc. pen.*, Torino, IV, 1990, 105; in giurisprudenza cfr. Corte giust. 5 maggio 1979, in *Racc. giur. Corte*, 1979, 1642, e, da ultimo, Corte giust. 13 novembre 1993, in *Foro it.*, 1993, IV, 173.

[30] Anche la normativa tedesca, che pure già estendeva al programma per elaboratore la tutela sul diritto d'autore, ha recepito le disposizioni della direttiva comunitaria attraverso la « *Zweites Gesetz zur Änderung von Vorschriften auf dem Gebiet des Urheberrechts* » del 9 giugno 1993: sul punto cfr. E. FADANI, Software *e diritto d'autore tedesco: dall'« Urheberrechtsgesetz » del 1965 al recepimento della direttiva n. 91/250/CEE*, in questa *Rivista*, 1994, 1039 ss.

[31] Cfr. GIANNANTONIO, *La tutela giuridica delle topografie dei prodotti a semiconduttori*, Padova, 1990; D. FONDAROLI, *Brevi note sulle norme per la tutela giuridica delle topografie dei prodotti a semiconduttori (legge 21 febbraio 1989, n. 70)*, in *Riv. trim. dir. pen. econ.*, 1991, 1045; critico sul punto PICOTTI, *Studi di diritto penale dell'informatica*, cit., 8, nt. 11.

[32] RISTUCCIA - ZENO ZENCOVICH, *Il* software *nella dottrina, nella giurisprudenza e nel d.lgs. n. 518/1992*, Padova, 2ª ed., 1993; R. RINALDI, *La disciplina penale del* software *nel decreto legislativo di attuazione della direttiva n. 91/250/CEE*, in *Legisl. pen.*, 1993, 781; D. FONDAROLI, *Osservazioni intorno ad alcune norme contenute nella recente normativa italiana sui* computer crimes, in L. SOLA - D. FONDAROLI, *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Bologna (Clueb), 1995, 32 ss.

quanto previsto dall'art. 171-*bis* », inserito dall'art. 9 del d.lgs. n. 518/1992 nella premessa dell'art. 171 stesso[33].

Vedremo tra breve entro quali termini opera attualmente l'art. 171 l.a. in ordine alle ipotesi di c.d. criminalità informatica.

Il delitto di cui all'art. 171-*bis*, di competenza pretorile, è reato comune, potendo essere commesso da « chiunque ».

Diverse sono le condotte punite, sorrette tutte dalla finalità di lucro. Si sanziona (con la pena della reclusione da tre mesi a tre anni e con la multa da L. 500.000 a L. 6.000.000): *a*) la duplicazione abusiva di programmi per elaboratori; *b*) la importazione, distribuzione, vendita, detenzione a scopo commerciale o concessione in locazione dei programmi, « sapendo o avendo modo di sapere che si tratta di copie non autorizzate »; *c*) il fatto concernente « qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore » (art. 171-*bis* prima e seconda parte).

Poche osservazioni in dettaglio.

La « duplicazione abusiva » è contraddistinta da un requisito di antigiuridicità speciale, che richiede un accertamento sulla legge extrapenale circa la disciplina della riproduzione lecita dei programmi.

Le condotte di « diffusione » (importazione, distribuzione ecc.) integrano gli estremi del reato se (oltre agli altri requisiti menzionati) il soggetto attivo « sa » o « ha modo di sapere » che si tratta di copie non autorizzate. Deve quindi ricorrere la consapevolezza della assenza di autorizzazione alla diffusione o, quanto meno, una mancata conoscenza colposa della mancanza di tale autorizzazione.

Più complessa l'interpretazione del contenuto della seconda parte dell'art. 171-*bis*, che punisce direttamente non una condotta, ma il « fatto » che « concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per l'elaboratore ».

L'indeterminatezza della fattispecie appare manifesta e contrasta con il principio di tassatività[34] riconosciuto dall'art. 25 della Costituzione.

Una circostanza aggravante, dalla cui applicazione consegue l'applicazione di una pena determinata in misura indipendente dalla pena base (pena non inferiore nel minimo a sei mesi di reclusione e multa a L. 1.000.000), è contemplata dalla terza parte dell'art. 171-*bis* per l'ipotesi in cui il fatto sia di particolare gravità, oppure qualora il programma oggetto della condotta sanzionata (abusiva duplicazione, importazione, distribuzione, vendita, detenzione a scopo commerciale o locazione) sia stato precedentemente « distribuito, venduto o concesso in locazione su supporti contrassegnati dalla SIAE». Quest'ultima disposizione è complementare alla integrazione dell'art. 103 l.d.a. (operata dall'art. 6, d.lgs. n. 518/1992), che estende ai programmi per elaboratore la tutela garantita dalla legge sul diritto d'autore attraverso l'iscrizione nel registro pubblico

---

[33] La tutela prestata dalla novella si applica anche ai programmi creati prima della entrata in vigore della stessa, fatti salvi gli eventuali atti conclusi e i diritti acquisiti anteriormente a tale data (art. 199-*bis* l.d.a., modificato dall'art. 11, d.lgs. n. 518/1992); A. LANZI, *Commento agli artt. 9 e 10*, in *Commentario* a cura di V. FRANCESCHELLI, in *Le nuove leggi civili commentate*, 1995, 314 ss..

[34] F. BRICOLA, voce *Teoria generale del reato*, cit., 46.

speciale, il quale fa fede, sino a prova contraria, dell'esistenza dell'opera e del fatto della sua pubblicazione (art. 103, comma 5).

La previsione della circostanza aggravante sottolinea la maggiore gravità della lesione al bene giuridico protetto, quando i fatti incriminati concernino programmi già registrati, ovvero programmi la cui paternità e struttura risulta formalmente documentata per assicurare una tutela rafforzata.

Il comma 2 dell'art. 171-*bis* stabilisce la pena accessoria della pubblicazione della sentenza di condanna (anche per la fattispecie base) in uno o più quotidiani e in uno o più periodici specializzati.

L'art. 172 l.d.a., non modificato dal d.lgs. n. 518/1992, prevede una ipotesi colposa punita con sanzione amministrativa. Il disposto fa riferimento letteralmente ai « fatti preveduti nell'articolo precedente », alludendo con tutta evidenzia all'art. 171, e non certo all'art. 171-*bis*, soltanto di recente inserito nel tessuto normativo ed ignoto al legislatore del 1941.

D'altronde pare difficilmente immaginabile una figura colposa di duplicazione e di diffusione del programma, stante la particolare descrizione del « fatto » punibile contenuta nell'art. 171-*bis* (mentre naturalmente il discorso sarebbe diverso in relazione ad ipotesi « altre », per esempio, di manipolazione). Necessaria appare comunque una norma di raccordo che fughi eventuali perplessità.

Come anticipato, per il programma per elaboratore, una volta presupposto l'inserimento del programma tra le opere dell'ingegno, residua un margine di applicabilità per l'ipotesi di cui all'art. 171 l.d.a., che pure riguarda la duplicazione e diffusione illecita delle opere dell'ingegno, senza distinzione di sorta.

In particolare, il dettato dell'art. 171 si presta a disciplinare le ipotesi di duplicazione e di diffusione del programma stesso non orientata ai fini di lucro (come invece espressamente richiesto dall'art. 171-*bis*), ma realizzata « senza averne diritto, a qualsiasi scopo e in qualsiasi forma » (pertanto, anche le condotte poste in essere a titolo gratuito, di cortesia o di mera amicizia). Per tale fattispecie la pena prevista è la sola multa (da L. 100.000 a L. 4.000.000) salva l'ipotesi aggravata di cui all'ultimo comma dell'art. 171 (pena alternativa della reclusione fino ad un anno o della multa non inferiore a L. 1.000.000) se i reati sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

3. I PRINCIPI DELLA LEGGE N. 547/1993.

Il patrimonio informatico, inteso come complesso di informazioni e di sistemi elettronici per la memoria e la elaborazione dei dati stessi, pur non ricevendo tutela rispetto alle modalità di aggressione peculiari del furto — piuttosto si è visto che esso è assoggettato alla disciplina relativa alla proprietà intellettuale[35] — viene tuttavia protetto sotto altri profili, quali il danneggiamento.

[35] Sul punto cfr. par. precedente.

La legge sulla criminalità informatica n. 547/1993 del 23 dicembre 1993, infatti, non prende in considerazione tutte le tipologie di aggressione ai dati e programmi informatici, intesi come « patrimonio », ma soltanto alcune di esse.

Innanzi tutto si è accantonata l'idea di individuare il nuovo bene giuridico della « intangibilità informatica », suggerito da parte della dottrina come autonomo e nuovo bene da aggiungere al novero dei beni giuridici meritevoli di tutela penale[36].

Né tanto meno si è seguita la strada della individuazione di una nuova ed autonoma « grandezza di base », accanto alla Materia ed alla Energia[37], da identificare nell'« Informazione »[38], costituente strumento di potere e fonte potenziale di pericolosità[39].

Il legislatore, invece, ha optato per un intervento « ortopedico », realizzato attraverso il mero adeguamento del codice penale vigente alle nuove esigenze di tutela, sulla falsariga della legislazione tedesca[40], rinunciando con ciò al modello francese[41], che prevede un *corpus* di norme (comunque — si badi bene — inserite nel tessuto nel Codice Penale) riservate alla sola criminalità informatica.

Insomma, non si è creato un microsistema interno al sistema penale generale, ma si è cercato di adeguare le singole fattispecie ai casi esaminati dalla giurisprudenza.

4. La tutela del patrimonio informatico.

a) La denegata ipotesi del furto di dati, informazioni e programmi.

Nel contesto in esame, e stante i presupposti evidenziati, non si rinviene una norma atta a punire il furto di dati, che si tradurrebbe in una forma di furto di informazioni, come evidenziato da parte della dottrina[42].

---

[36] V. Militello, *Informatica e criminalità organizzata*, in *Riv. trim. dir. proc. pen.*, 1990, 85.

[37] In tal senso Steinbuch, in *Gewerblicher Rechtsschutz und Urheberrecht*, 1987, 581.

[38] U. Sieber, *Computer Crimes and other crimes related to Information Technology. Commentary and Preparatory Questions for the Colloquium of the AIDP to be organized in Würzburg*, 5-8 ottobre 1992; Id., *Informationsrecht und Recht der Informationstechnik*, in NJW, 1989, 2569 ss.

[39] U. Sieber, *Computerkriminalität*, cit., 111.

[40] Si tratta della *Seconda legge sulla criminalità economica della Repubblica Federale tedesca* del 15 maggio 1986, approfonditamente commentata da L. Picotti, *Studi di diritto penale dell'informatica*, cit., 33.

[41] Prima attraverso la legge n. 88/19 del 5 gennaio 1988 relativa alla frode informatica, che ha introdotto nel previgente Codice Penale francese del 1810 il Capo III del Titolo II del Libro Terzo, gli artt. da 462.2 a 462.9, sotto la rubrica « Di certi illeciti in materia informatica »; poi con la legge n. 92/685, che, insieme ad altri provvedimenti legislativi, ha sostituito il dettato del Codice Penale. Anche in quest'ultima normativa si è continuato a dedicare alla criminalità informatica il Capo III, Titolo II, Libro III, relativo alle « Lesioni del sistema di elaborazione automatizzata di dati » — artt. da 323.1 a 323.7. Per alcune considerazioni sulla normativa francese cfr. D. Fondaroli, *I problemi della criminalità informatica e la legge francese n. 88/19 del 5 gennaio 1988*, cit., 762 ss.; M. Mantovani, *I reati informatici nella recente legge francese: l'uso e l'accesso abusivi*, cit., 885 ss.

[42] M.P. Lucas de Leyssac, *Il furto di informazione*, cit., 625.

L'unica forma di « approvazione » di dati o informazioni o programmi sanzionata, pertanto, resta quella della duplicazione e diffusione contemplata dalla legge sul diritto d'autore, per la quale si rinvia al par. 2.

*b) Il danneggiamento di sistemi informatici e telematici (art. 635-*bis *cod. pen.) e l'attentato a impianti di pubblica utilità (art. 420 cod. pen.).*

Al contrario, la legge n. 547/1993 ha arricchito di nuovi contenuti le fattispecie penali codificate attraverso un intervento, per così dire, a « macchia di leopardo ».

Vengono sanzionate, così, le condotte di *danneggiamento* che abbiano ad oggetto altrui sistemi informatici o telematici, ovvero programmi, informazioni o dati.

In particolare, la legge n. 547/1993 ha introdotto nel Codice Penale l'art. 635-*bis* (art. 9) ed ha sostituito il dettato dell'art. 420 cod.pen. (art. 2).

In primis una precisazione di carattere generale: il legislatore non solo non offre una definizione della maggior parte dei concetti « tecnici » richiamati dalle singole disposizioni, ma addirittura utilizza ed assimila espressioni generiche, quali, ad esempio, « informatica e telematica »[43].

La prima disposizione (art. 635-*bis* cod. pen.) rappresenta un mero adeguamento della disciplina del danneggiamento « comune » al fine di assoggettare a pena le azioni incidenti su sistemi informatici e telematici.

Le condotte punite, infatti, sono quasi le medesime (distruggere, deteriorare, rendere in tutto o in parte inservibili) previste anche dall'art. 635 cod. pen.[44]. Soltanto della « dispersione » non si fa menzione nell'art. 635-*bis* cod. pen., probabilmente in considerazione della incopatibilità di tale condotta con la natura dei « beni informatici »[45].

L'oggetto « materiale » preso in considerazione da quest'ultima norma consiste in un bene « immateriale » e pertanto di natura ben diversa dalle cose « mobili o immobili » di cui all'art. 635 cod. pen.

Come per l'art. 635 cod. pen., il legislatore ha statuito che la fattispecie sia sussidiaria rispetto ai « più gravi » reati[46].

---

[43] A. Rossi Vannini, *La criminalità informatica*, cit., 430 s.

[44] Analoghe condotte (« chi illegittimamente cancella, sopprime, rende inutilizzabili o manomette dati ») sono punite dal par. 303a StGB, che, da un lato, richiede anche una clausola di « illiceità speciale », dall'altro non esige il requisito della altruità della cosa: diffusamente a riguardo L. Picotti, *Studi di diritto penale dell'informatica*, cit., 68 ss. La legge francese n. 88-19 del 5 gennaio 1988 aveva introdotto una ipotesi di « danneggiamento » imperniata sulla introduzione, soppressione o modificazione di dati (art. 462-4 cod. pén.), che però, facendo riferimento nella seconda parte anche ai modi di elaborazione e di trasmissione, presentava profili di commistione con la disciplina del sabotaggio (art. 462-3 cod. pén.). La elaborazione del nuovo Codice Penale ha favorito la rilettura (anche) della normativa informatica, accorpando le due diverse condotte del danneggiamento (art. 323-2 cod. pén.), relativo alla alterazione fraudolenta dei meri dati informatici, e del sabotaggio informatico (art. 323-3), concernente la manipolazione del sistema di elaborazione automatizzata.

[45] Sul punto cfr. L. Sola, *Prime considerazioni in merito alla legge n. 547/1993*, in L. Sola - D. Fondaroli, *La nuova normativa in tema di criminalità informatica*, cit., 13.

[46] Utili indicazioni sull'individuazione del concetto di « reato più grave » possono essere tratte dall'interpretazione dell'art. 81 cod. pen., che richiama una locuzione analoga; a riguardo per tutti cfr. M. Romano, sub *art. 81*, in *Commentario sistematico del Codice Penale*, I, Milano, 2ª ed., 1995, par. 12, 713 s.

Una particolare circostanza aggravante (che comporta la pena della reclusione da uno a quattro anni) è prevista dal comma 2 della disposizione che disciplina il caso in cui il fatto sia commesso « con abuso della qualità di operatore del sistema ».

Si tratta di una circostanza equiparabile alle circostanze ad efficacia speciale[47] per la quale la pena è determinata in misura indipendente dalla pena base.

Il rilievo non è di poco conto se si pensa che le circostanze per le quali la legge stabilisce una pena diversa da quella ordinaria e quelle ad efficacia speciale, a differenza delle circostanze ad efficacia comune, sono le uniche ad essere prese in considerazione ai fini della determinazione della competenza per materia (art. 4 cod. proc. pen.) — che tuttavia nel caso di specie resta sempre del Pretore — e del computo della durata della custodia cautelare[48] (art. 278 cod. proc. pen.).

Particolarmente rilevante e significativa in tale contesto è l'ipotesi prevista dall'art. 420 cod. pen., che punisce l'*attentato agli impianti di pubblica utilità* (art. 420 cod. pen.), ovvero il fatto « diretto a danneggiare o distruggere impianti di pubblica utilità ».

Si tratta di fattispecie riconducibile al generale ambito del « sabotaggio informatico ».

Anche tale disposizione è stata modificata dalla legge n. 547/1993 (art. 2), che ha sostituito il dettato originario, adeguando la disposizione alle esigenze di tutela cui la legge sulla criminalità informatica tende a dare una risposta.

La novella, infatti, ha inserito tra il primo e il secondo comma dell'art. 420 cod. pen. un nuovo comma, con il quale si incrimina il « fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti ».

In effetti il dettato precedente la riforma del 1993 concerneva condotte aventi ad oggetto « impianti » intesi nella accezione letterale del termine, spiccatamente agganciata ad un bene materiale[49]. La nuova formulazione della disposizione tiene conto della immaterialità congenita dei dati e delle informazioni, nonché dei programmi che questi elaborano, per cui la disciplina attuale afferisce al « fatto diretto a danneggiare o distruggere » sia impianti di pubblica utilità, sia sistemi informatici o telematici di pubblica utilità, sia dati, informazioni o programmi in essi contenuti o ad essi pertinenti.

L'ipotesi è strutturata come fattispecie di attentato, incentrandosi sulla punizione del « *fatto diretto a* » produrre determinati risultati. Essa si distingue dalle tipologie di sabotaggio previste da altri ordinamenti, inte-

---

[47] T. PADOVANI, voce *Circostanze del reato*, in *Dig. disc. pen.*, Torino, II, 1988, 210.

[48] A quest'ultimo riguardo si deve tener conto anche della attenuante *ex* art. 62, n. 4, cod. pen. e della recidiva di cui all'art. 99, comma 4, cod. pen.

[49] L. SOLA, *I computers nell'ordinamento giuridico italiano: alcune considerazioni*, in L. SOLA - D. FONDAROLI, *A proposito della criminalità informatica*, cit., 15. Nonostante la prevalente interpretazione dottrinale nel senso espresso nel testo, una nota pronuncia giurisprudenziale ha ritenuto applicabile la fattispecie ad un caso di manipolazione di dati, intendendo in senso lato il concetto di « impianto » ed interpretando lo stesso come « sistema » (Trib. Firenze, Uff. Istr., 27 gennaio 1986, in questa *Rivista*, 1986, 962).

grate, ad esempio, dal *fatto di* disturbare un procedimento di una elaborazione dati (di essenziale significato per una impresa o azienda altrui o per una Pubblica Amministrazione), mediante manomissione di dati (*ex* par. 202a StGB), oppure distruzione, danneggiamento, manomissione o rimozione di un impianto di elaborazione automatica o di un supporto di dati[50] (par. 303b StGB); ovvero, dal *fatto di* ostacolare o falsificare il funzionamento di una elaborazione automatizzata di dati[51] (art. 323-2 cod. pen. francese).

La fattispecie di cui all'art. 420 cod. pen., come si è anticipato, costituisce un reato di attentato, che per sua stessa natura suggella una anticipazione della soglia della punibilità: la consumazione del reato, infatti, si verifica allorché vengono posti in essere gli « atti diretti a ».

La norma consente un aggravamento di pena per caso in cui dal fatto (di attentato) derivi la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema. In tal caso la pena è della reclusione da tre a otto anni (art. 420, comma 3, cod. pen.).

Si tratta di una fattispecie riconducibile al novero dei reati aggravati o qualificati dall'evento, ovvero degli illeciti in relazione ai quali la realizzazione di un fatto ulteriore rispetto a quello voluto determina un aggravamento di pena. L'evento ulteriore è posto a carico dell'agente se non voluto, ma « oggettivamente realizzato » oppure, secondo quella che è l'interpretazione più garantista[52] se posto in essere con colpa.

Al contrario, se la distruzione o il danneggiamento è voluto (e se quindi l'elemento psicologico consiste nel dolo di danneggiamento), troverà applicazione la norma che punisce la condotta dolosa di cui all'art. 635-*bis* cod. pen..

Quanto premesso evidenzia la rilevanza dell'accertamento dell'elemento psicologico per la individuazione della fattispecie concretamente applicabile.

5. *(segue)* LA TRUFFA INFORMATICA.

L'art. 10 della legge n. 547/1993 ha inserito nel tessuto delle norme penali in tema di truffa una specifica ipotesi di frode informatica.

La *ratio* della disposizione discende dalla difficoltà di applicazione della fattispecie tradizionale di truffa (art. 640 cod. pen.) nel caso in cui la medesima venga perpetrata attraverso l'impiego di tecniche informatiche o telematiche.

Si tratta di una fattispecie formulata in modo generico e vago che si ispira alla ipotesi di truffa mediante *computer* disciplinata dall'ordinamento penale tedesco (part. 263a StGB), la quale descrive una fattispecie

[50] Analizza con attenzione la disciplina in materia L. PICOTTI, *Studi di diritto penale dell'informatica*, cit., 72 ss.

[51] Sul contenuto della norma originaria (art. 462-3 cod. pén.) introdotta dalla legge n. 88-19 si veda D. FONDAROLI, *I problemi della criminalità informatica*, cit., 801. Si veda anche anche *supra* nt. 41.

[52] Sul punto cfr. F. MANTOVANI, *Diritto penale. Parte generale*, Padova, 3ª ed., 1992, 390; G. FIANDACA - E. MUSCO, *Diritto penale. Parte generale*, Bologna, 3ª ed., 1995, 588 s.

« aperta », tale da abbracciare ogni possibile intervento sia sull'*input*, sia sul programma, sia sulla *consolle*[53]: tale fattispecie ha confini così dilatati, che attraverso la previsione della condotta di « utilizzazione non autorizzata di dati, finalizzata a procurare a sé o ad altri un vantaggio patrimoniale illecito » e « danneggiamento » del patrimonio altrui influendo sul risultato di un procedimento di elaborazione automatica di dati, è possibile punire gli « abusi » attraverso il Bancomat[54].

L'art. 640-*ter* cod. pen. sanziona con la pena della reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno[55].

La struttura è per certi versi analoga a quella dell'art. 640 cod. pen., ma tiene conto del fatto che quest'ultimo richiede il requisito della induzione in errore di taluno: l'interpretazione unanime della giurisprudenza, infatti, è nel senso di ritenere che il pronome personale non possa non riferirsi ad una persona fisica. La nuova norma pare perciò importante lad-

---

[53] Ampiamente sulla truffa mediante *computer* nell'ordinamento penale tedesco cfr. L. PICOTTI, *Studi di diritto penale dell'informatica*, cit., 49 ss. Parte del dibattito attuale concerne la possibilità di ricondurre al par. 263a StGB qualunque uso illecito di strumentazione elettronica, il cui risultato incida sulla modificazione del patrimonio: in senso positivo, ad esempio, cfr. BGH 10 novembre 1994, in BGHSt, 40, 331 ss. (tra i commenti alla sentenza cfr. R. GRANDERATH, *BGH: Leerspielen von Geldspielautomaten*, in *Computer und Recht*, 1995, 169 s.); si veda anche BayObLG, 10 febbraio 1994, in *NJW*, 1994, 960 ss.: OLG Celle 11 aprile 1989, in *NStZ*, 1989, 367 ss. C. BÜHLER, *Die strafrechtliche Erfassung des Mißbrauchs von Geldspielautomaten*, Heidelberg, 1995. La disciplina francese conosce ipotesi di manipolazione di dati (rispettivamente di « sabotaggio » e di « danneggiamento » informatico) che non contemplano né il fine di profitto, né il requisito del danno al patrimonio altrui: attualmente la disciplina è contemplata dagli artt. 323-2 e 323-3 cod. pén., che ha sostituito gli artt. 462-4 e 462-5 contenuti nella legge n. 88-19 del 5 gennaio 1988, che ha introdotto per la prima volta la normativa relativa alla frode informatica nel Codice Penale: cfr. D. FONDAROLI, *I problemi della criminalità informatica e la legge francese n. 88-19 del 5 gennaio 1988*, cit., 793 ss.

[54] Cfr. ancora L. PICOTTI, *Studi di diritto penale dell'informatica*, cit., 54; circa la frode attraverso il Bancomat si veda nel testo *infra* par. 10.

[55] La fattispecie è aggravata e determina l'applicazione della reclusione da uno a cinque anni e della multa da lire seicentomila a lire tre milioni se il fatto è commesso a danno dello Stato o di altro Ente pubblico o col pretesto di far esonerare taluno dal servizio militare (art. 640, comma 2, n. 1, cod. pen., richiamato dall'art. 640-*ter*, comma 2, cod. pen.), ovvero se il fatto è commesso con abuso delle qualità di operatore del sistema (art. 640-*ter* comma 2, cod. pen.). Il delitto è di competenza del Pretore nella ipotesi base, del Tribunale nelle ipotesi aggravate. A riguardo può sorgere la necessità di un chiarimento legislativo: nel caso in cui ricorrano le richiamate circostanze aggravanti *ex* art. 640, comma 2, cod. pen., l'art. 7, lett. *m*), cod. proc. pen. prevede la competenza del Pretore. È anche vero, tuttavia, che l'art. 7 cod. proc. pen. si riferisce alla mera truffa aggravata *ex* art. 640, comma 2, cod. pen., mentre l'art. 640-*ter* afferisce ad un diverso ed autonomo delitto, che è la frode informatica. Si tratta di verificare se la volontà del legislatore di derogare alla disciplina sulla competenza vada riferita alla mera « truffa aggravata *ex* art. 640, comma 2, cod. pen. », oppure se essa afferisca ad ogni ipotesi che richiami (anche soltanto) *per relationem* le circostanze aggravanti di cui al comma 2 dell'art. 640 cod. pen.

La perseguibilità del reato è a querela per la fattispecie base, d'ufficio in tutte le altre ipotesi in cui ricorra una circostanza aggravante, anche diversa da quella prevista dal comma 2 dell'art. 640-*ter* (art. 640-*ter*, comma 3, cod. pen.).

dove non sia possibile individuare un soggetto « vittima » della induzione in errore: situazione che si verifica puntualmente quando si realizzano gli estremi della truffa, in tal caso avendo l'autore come interlocutore il solo elaboratore.

Per superare l'*impasse*, ostativo alla applicazione della fattispecie per la violazione del divieto di analogia in materia penale[56], il legislatore ha descritto la condotta *ex* art. 640-*ter* cod.pen. in termini di « alterazione in qualsiasi modo » effettuata del funzionamento del sistema, o di intervento senza diritto con qualsiasi modalità su dati o programmi contenuti in un sistema informatico.

La condotta, che vorrebbe assumere connotazioni prettamente oggettive, difetta sul piano della determinatezza, che pure è principio essenziale nella creazione delle fattispecie penali[57]. Le caratteristiche della « alterazione », infatti, non sono definite né circoscritte, per cui la condotta stessa diviene fatiscente. Anche in questa ipotesi, come in altre di recente conio legislativo — peraltro di struttura di versa, il « fatto » ed il suo disvalore tendono a scomparire[58].

La necessità della induzione in errore di taluno (art. 640 cod. pen.) è superata, mentre il disvalore della fattispecie si incentra nella qualificazione della condotta di alterazione del sistema, definita come alterazione compiuta « senza diritto », ovvero non autorizzata dal « titolare del sistema » o da colui che ne è comunque responsabile.

6. La tutela della riservatezza dei dati informatici: una lacuna legislativa prossima ad essere colmata.

La tutela della « riservatezza » delle informazioni contenute nei dati informatici, se si eccettuano alcune frammentarie disposizioni[59], è quasi unicamente affidato alle disposizioni relative alla libertà personale, contenute nella legge n. 547/1993.

Fino ad ora, infatti, nessuno dei Progetti di legge presentati in materia di « riservatezza delle informazioni » è sfociato in un provvedimento legislativo, sebbene proprio dalle esigenze di tutela della personalità abbia preso avvio la discussione circa il problema della aggressione alla vita privata[60].

[56] Per tutti cfr. F. Bricola, voce *Teoria generale del reato*, cit., 46.

[57] Sul punto cfr. F. Bricola, *La discrezionalità nel diritto penale*, Milano, 1965, 277; F. Palazzo, *Il principio di determinatezza nel diritto penale*, Padova, 1979, 32; Id., voce *Legge penale*, in *Dig. disc. pen.*, Torino, VII, 1993, 355.

[58] F. Sgubbi, *Il reato come rischio sociale*, Bologna, 1990, 52.

[59] Si pensi all'art. 8, comma 4, legge 1 aprile 1981, n. 121, sul nuovo ordinamento di pubblica sicurezza; agli artt. 4 e 8 della legge n. 300/1970 contenente lo Statuto dei lavoratori all'art. 1 Delib. Consob 29 ottobre 1991, n. 5530 e artt. 25 e 14 l.n. 1/1991 in tema di tutela della riservatezza di dati relativi a titoli mobiliari. Per alcune considerazioni sul punto cfr. V. Mucaria, *Aspetti penalistici della regolamentazione delle banche dati*, in *Riv. pen.*, 1986, 931 ss.; G. Corrias Lucente, *Informatica e diritto penale: elementi per una comaprazione col diritto statunitense*, in questa *Rivista*, 1987, 547. Per alcune considerazioni circa la tutela della riservatezza cfr. *supra* par. 1.

[60] Ben diversa la situazione negli altri Paesi europei. In Francia la tutela della riservatezza è stata affidata dapprima alla legge n. 70/643, sanzionante — tra l'altro — la captazione sia di parole pronunciate da una persona in luogo privato, sia di immagini riprese nelle medesime condizioni,

Parte delle difficoltà a pervenire ad una soluzione normativa discende dalla contrapposizione dei diversi centri di interesse.

Infatti tali Disegni di legge, non escluso quello di recente proposto alla Camera dal Governo[61], non solo estendono le garanzie previste dalla legislazione comunitaria e dei singoli Paesi europei anche alle persone giuridiche, ma addirittura la disciplina è la medesima tanto per le persone fisiche quanto per quelle giridiche, con la conseguenza che essa, creata sul « modello » delle esigenze di tutela della persona fisica, appare inadeguata alla struttura della persona giuridica[62].

D'altronde la garanzia della riservatezza dei dati relativi alle persone giuridiche deve essere armonizzata con la necessità, tipica di alcuni settori delle relazioni sociali quali quello commerciale e societario, di trasparenza e di libertà della circolazione delle informazioni, e ciò nell'interesse sia di una leale concorrenza tra le imprese, sia della massa dei fruitori dei servizi. Una corretta impostazione delle soluzioni del problema richiede attenzione per contemperare le esigenze di pubblicità, forse prendendo anche in considerazione la eventualità di prevedere una differenziata disciplina per le persone fisiche, le persone giuridiche e le imprese. Queste ultime, invero, possono essere tanto persone fisiche quanto persone giuridiche: in entrambi i casi la sicurezza dei traffici commerciali e le esigenze di informazione dei consumatori impongono la garanzia della trasparenza delle informazioni.

In particolare la legge sulla disciplina delle banche dati dovrebbe tener conto di diversi fattori: la necessità, da un lato, di disporre di informazioni a fini di programmazione; dall'altro, di garantire la tutela dei diritti fondamentali del cittadino e delle persone giuridiche.

Non occorre sottolineare, infatti, che a prescindere dalla titolarità della banca dati, l'informazione descrive pur sempre un aspetto della « personalità »[63], intesa quale insieme delle caratteristiche peculiari di un soggetto, sia esso pubblico o privato: in quanto estrinsecazione della personalità, quindi, l'« informazione » dovrebbe essere autonomamente tute-

---

nonché la conservazione o divulgazione delle registrazioni o dei documenti ottenuti per mezzo di una di tali ipotesi delittuose (artt. 368 e 369: cfr. A. MANNA, *Tutela penale della personalità*, cit., 102 s.); poi alla legge n. 78-17 del 6 gennaio 1978 « relative à l'informatique, aux fichiers et aux libertès » (sul punto cfr. anche D. FONDAROLI, *I problemi della criminalità informatica*, cit., 765), recepita nella legge n. 92-684 del 22 luglio 1992 contenente la riforma delle disposizioni del Codice Penale relative alla repressione dei crimini e dei delitti contro le persone (artt. da 226-16 a 226-24 cod. pén.). Nella Repubblica Federale di Germania il riconoscimento del diritto alla « autodeterminazione dell'informazione » dei cittadini ottenne il primo riconoscimento con la decisione del *Bundesverfassungsgericht* 15 dicembre 1983, in *BVerGE*, 65, 1; cfr. anche U. SIEBER, *Computerkriminalität*, cit., 100; il « possesso » ed il godimento esclusivo dei « beni informatici » trova tutela nel par. 202a StGB: sul punto cfr. *infra* nel testo par. 9. Su un Progetto di Direttiva dell'Unione europea cfr. G. RÜPKE, *Aspekte zur Entwicklung eines EU-Datenschutzrechts*, in *ZRP*, 1995, 185 ss.

[61] Disegno di legge n. 1901 presentato il 9 gennaio 1995, XII Legislatura.

[62] Sulla riconoscibilità del diritto alla riservatezza alle persone giuridiche si veda CATAUDELLA, *Riservatezza (diritto alla), 1) diritto civile*, in *Enc. giur. Treccani*, XXVI, Roma, 1991, 5.

[63] In generale sulla tutela penale della personalità si veda A. MANNA, *Beni della personalità e limiti della protezione penale*, cit., *passim*; ID., *Tutela penale della personalità*, cit. 67 ss.; ID., *La protezione penale dei dati personali nel diritto italiano*, in *Riv. trim. dir. pen. econ.*, 1993, 179 ss.; anche con ampi riferimenti bibliografici cfr. A. ROSSI VANNINI, *La criminalità informatica*, cit., 435 ss.

lata[64]. I termini della questione vanno comunque tenuti distinti, poiché altro è la necessità di tutela della riservatezza delle persone, altro è l'opportunità di assoggettare ad autonoma garanzia la riservatezza delle informazioni[65].

Non solo. Il legislatore non può prescindere dalla valutazione dei contrapposti interessi, ovvero: per un verso, del diritto all'informazione, che si esplica nella duplice direzione del diritto ad informare e del diritto di essere informati ed è coperto da garanzia costituzionale attraverso l'art. 21; per l'altro, del diritto alla riservatezza, che trova fondamento negli artt. 2 e 3 della Costituzione[66].

Al perseguimento di tali finalità è orientato il Disegno di legge n. 1901 presentato dal Governo alla Camera dei deputati il 19 gennaio 1995 (XII legislatura), che contempla anche una serie di disposizioni di carattere penale, volte a punire le violazioni della disciplina contenuta nel Disegno di legge stessa (artt. 23 ss.).

Come si è detto, il nostro resta uno dei pochi Paesi europei a non prevedere una disciplina autonoma delle banche dati[67], nonostante la ratifica della citata Convenzione che regola la raccolta e conservazione di dati personali attraverso sistemi di elaborazione informatica[68]. Con la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[69], l'Unione Europea, sulla falsariga della legislazione già vigente in alcuni Paesi del Vecchio Continente ha dettagliatamente descritto la disciplina « minima » in tema di tutela della circolazione dei dati personali, con particolare attenzione ai profili di garanzia della riservatezza della persona « identificata o identificabile ».

Del resto la problematica delle banche dati e, più in generale, del rapporto tra diritto di informazione e tutela della riservatezza dei dati, appare strettamente connessa alla potenziale lesività della elaborazione informatica, che accentua i profili di pericolosità intrinsecamente connessi ad ogni forma di raccolta e conservazione di informazioni.

La maggiore quantità di notizie di cui i processi informatici consentono rapidamente sia di venire in possesso sia di diffondere, acquista un signi-

---

[64] U. Sieber, *Computerkriminalität*, cit., 111.

[65] L. Picotti, *Studi di diritto penale dell'informatica*, cit., 76, evidenzia bene i due aspetti della questione, in relazione alla disciplina penale tedesca della tutela della riservatezza dei dati informatici (par. 202a StGB) e delle persone (par. 41 BDSG). Lo Schema di legge delega per la riforma del Codice Penale (in *Documenti Giustizia*, 1992, 3, 372) distingue, nella « nuova categoria dei reati contro la riservatezza bene emergente della personalità umana ed oggetto di crescenti forme di aggressione », i reati contro la riservatezza della vita privata dai reati contro la riservatezza delle comunicazioni.

[66] G. Giacobbe, voce *Riservatezza*, in *Enc. dir.*, Milano, XL, 1989, 255.

[67] La legge spagnola (29 ottobre 1992, n. 5) è denominata « Lortad » (cfr. in questa *Rivista*, 1994, 117): si veda M.G. Losano, *La legge spagnola sulla protezione dei dati personali*, in questa *Rivista*, 1993, 867 ss.; per la normativa francese cfr. *supra* nt. 60.

[68] Convenzione di Strasburgo dell'8 gennaio 1981, ratificata dall'Italia con legge 21 febbraio 1989, n. 98. Particolarmente interessante appare anche una proposta di Direttiva dell'Unione Europea: cfr. G. Mirabelli, *In tema di tutela dei dati personali (note a margine della proposta modificata di Direttiva CEE)*, in questa *Rivista*, 1993, 609).

[69] Cfr. in *Gazzetta Ufficiale delle Comunità Europee*, N.L. 281/31 ss. del 23 novembre 1995. Al punto (27) dei *Considerando* (N. L 281/33) si precisa che la tutela va applicata al trattamento sia automatizzato, sia *manuale*.

ficato di natura anche valutativa: essa infatti fornisce una immagine « a tutto tondo » del soggetto cui le informazioni afferiscono, decuplicando l'area del rischio di lesività della sfera privata ad opera di soggetti terzi[70].

A fronte di tale situazione si propone di riconoscere al « patrimonio spirituale », ai « diritti della personalità » ed ai « diritti di accesso all'informazione » natura di autonomi beni giuridici, meritevoli di tutela penale[71].

Non che ciò debba corrispondere ad una dilatazione indifferenziata della sfera di applicazione delle garanzie penali a discapito del principio del diritto penale quale *extrema ratio*. Anzi: in taluni ambiti, soprattutto in quello della c.d. criminalità economica, nel quale il legislatore ha fatto confluire molte fattispecie di c.d. criminalità informatica[72], le alternative di tutela possono trovare ampio spazio di applicazione nell'ambito civile ed amministrativo, così da consentire il recupero della conformità del diritto penale al principio di « frammentarietà » e « sussidiarietà »[73].

Per converso, si fa osservare che la attuale « civiltà del rischio » induce alla individuazione di nuovi beni superindividuali, quali appunto quelli citati, che fanno dubitare, per la potenziale pericolosità conseguente alla loro intrinseca indeterminatezza, della opportunità della estensione del cono della protezione penale.

Anche sotto tale profilo, sempre più fondato pare il rilievo della dottrina nel senso del riconoscimento di una mera funzione simbolica al diritto penale[74].

7. *(segue)* a) L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO.

La legge n. 547/1993 offre una tutela prodromica della riservatezza attraverso la introduzione della fattispecie di accesso non autorizzato all'elaboratore (art. 615-*bis* cod. pen.) e le norme dirette a proteggere l'inviolabilità delle comunicazioni informatiche (artt. 617-*quater*, 617-*quinquies* e 617-*sexies* cod. pen.).

---

[70] Sui complessi risvolti dell'aggressione dei diritti della personalità cfr. A. MANNA, *Tutela penale della personalità*, cit., 124; ID., *Beni della personalità e limiti della protezione penale*, cit., 177 ss.

[71] U. SIEBER, *Computerkriminalität*, cit., 111 s. Diffusamente sul punto A. MANNA, *Beni della personalità e limiti della protezione penale*, cit., 430 ss.

[72] Pare interessante osservare che la disciplina tedesca in tema di criminalità informatica è contenuta proprio nella Seconda Legge per la lotta contro la *criminalità economica* (2.WiKG) del 15 maggio 1986, che ha accolto alcuni spunti propri della dottrina tedesca risalenti alla fine degli anni Settanta: cfr. L. PICOTTI, *Studi di diritto penale ell'informatica*, cit., 16. Circa il dibattito sulla opportunità di ricondurre la criminalità informatica all'alveo della criminalità economica cfr. C. BÜHLER, *Die strafrechtliche Erfassung des Mißbrauchs von Geldspielenautomaten*, cit., 5; W. BOTTKE, *Empfiehlt es sich, die strafrechtliche Verantwortlichkeit für Wissenwschaftsstraftaten zu verstärken?*, in *wistra*, 1991, 81.

[73] Per tutti cfr. A. MANNA, *Tutela penale della personalità*, cit., 23 ss. La dottrina, tuttavia, non può non rilevare che, al contrario, la tendenza attuale del legislatore, è nel senso della completezza ed omnicomprensività del diritto penale: W. HASSEMER, *Kennezeichen und Krisen des modernen Strafrechts*, in *ZRP*, 1992, 381.

[74] W. HASSEMER, *Kennezeichen und Krisen des modernen Strafrechts*, cit., 382; M. VOß, *Symbolische Gesetzgebung*, Ebelsbach, 1989, 181 ss.

Al problema della « necessità » di garantire tutela penale al diritto alla riservatezza si è già accennato[75].

Con la disposizione sull'accesso non autorizzato all'elaboratore il legislatore italiano si è adeguato alle indicazioni della normativa europea, mutuando l'analoga disposizione presente nel Codice Penale francese (art. 323.1 cod. pén.)[76].

Già lo Schema di delega legislativa per la forma del Codice Penale italiano, nell'ambito del più generale riconoscimento della tutela penale del diritto alla riservatezza, prevedeva una « direttiva » nel senso della incriminazione dell'« accesso abusivo ai sistemi informatici, consistente nel prendere cognizione di dati di un sitema informatico di elaborazione, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, sempre che il fatto non costituisca più grave reato »[77].

La normativa, configurando una ipotesi di pericolo astratto, si prefigge fra l'altro di scoraggiare le condotte degli *hackers* che, sebbene non necessariamente con dolo, comunque minacciano il corretto funzionamento degli elaboratori, la segretezza dei dati, la trasparenza del sistema informatico, l'integrità dei programmi.

L'art. 615-*ter* cod. pen., che si colloca nell'ambito della Sezione del Codice Penale relativo ai delitti contro l'inviolabilità del domicilio, punisce la condotta di accesso e di uso abusivo di un sistema informatico o telematico.

La norma fa seguito all'art. 615-*bis* cod. pen., inserito nel Codice Penale con la legge di riforma n. 98/1974, confermando l'orientamento legislativo a considerare le interferenze nella vita privata come un « prolungamento » della violazione di domicilio[78], inteso in senso lato non quale « luogo fisico », ma quale « proiezione spaziale della persona »[79].

La collocazione della disciplina dell'accesso ed uso non autorizzato nell'ambito della tutela per la inviolabilità del domicilio nonché la delimitazione della tipologia di condotte sanzionate, lascia intendere che il sistema informatico è considerato come « luogo » (in senso figurativo), come « sfera domestica », « situazione privata » in cui si esprime la personalità del soggetto e dalla quale resta escluso ogni estraneo[80] (salvo esplicite eccezioni).

Che, quindi, il legislatore non intenda riconoscere un diritto alla inviolabilità della vita privata e dei segreti, ossia un vero e proprio *Indiskretionsdelikt*[81], con il quale il bene « riservatezza » si affranchi dalla tutela ga-

---

[75] Cfr. *supra* par. 1.

[76] Sulle nuove disposizioni del vigente codice penale francese in tema di accesso ed uso non autorizzato dell'elaboratore cfr. D. Fondaroli, *I problemi della c.d. criminalità informatica*, cit., 787 s.; M. Mantovani, *I reati informatici nella recente esperienza francese: l'uso e l'accesso abusivi*, cit., 885 ss. Nel Regno Unito l'art. 1 del *Computer Misuses Act* punisce il « far seguire una qualsiasi funzione ad un computer con l'intenzione di garantirsi l'accesso a qualsiasi dato o programma contenuto in un qualsiasi computer: sul punto cfr. G. Tizzoni, *Regno Unito: « computer Misuse » o abuso di computer*, in Dir. pen. processo, 1995, 1337 ss..

[77] Cfr. art. 76-6, in *Documenti Giustizia*, cit., 424.

[78] F. Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in Aa.Vv., *Il diritto alla riservatezza e la sua tutela penale*, Milano, 1970, 15; A. Manna, *Tutela della personalità*, cit., 12; Id., *Beni della personalità e limiti della protezione penale*, cit., 294 ss.

[79] A. Rossi Vannini, *La criminalità informatica*, cit., 431.

[80] F. Pazienza, voce *Domicilio (delitti contro)*, in *Enc. Giur. Treccani*, Roma, XII, 1990.

[81] Circa la prospettiva tedesca cfr. A. Manna, *Tutela della personalità*, cit., 96 ss.; Maurach - Schröder - Mainwald, *Strafrecht-Besonderer Teil*, Heidelbeg 8. Aufl., 1995, 255 s.

rantita all'« onore » (per confluire in una sorta di « sfera della pace privata »), sembra quindi ormai una realtà con cui fare i conti.

L'« abuso » di cui trattasi discende da una clausola di antigiuridicità che estende l'oggetto dell'interpretazione della norma anche alla normativa extrapenale, cui è demandato il compito di regolare l'accesso « lecito » al sistema di elaborazione.

L'accesso abusivo, quindi, si realizza innanzi tutto quando il soggetto non è autorizzato ad « introdursi », ad entrare in contatto con il sistema stesso.

La seconda condotta incriminata consiste nel mantenimento non autorizzato. Essa si configura quando il soggetto è stato autorizzato all'accesso all'elaboratore, ma travalica i limiti di tale autorizzazione (per esempio utilizzando il sistema in tempi diversi da quelli stabiliti o per fini differenti dagli scopi cui il sistema è preordinato o per i quali l'agente è autorizzato ad utilizzare il sistema), per cui ciò che in realtà si punisce attraverso tale modalità di condotta è l'*uso* dell'elaboratore, o meglio del sistema, più che l'accesso ad esso.

La dizione della norma riecheggia le condotte punite dall'art. 614 cod. pen., ovvero la violazione del domicilio, che è ritenuta realizzarsi quando l'agente « si introduce » o si « trattiene » nei luoghi di privata dimora. Entrambe le condotte sono caratterizzate da un elevato grado di arretramento della soglia di punibilità.

Quanto alla determinazione della connotazione di « abuso », occorre osservare che la volontà di esclusione degli altri da parte del *dominus* del sistema può essere anche tacita, ma deve comunque essere identificabile.

Proprio per sottolineare la stretta connessione tra « titolarità » del sistema (nel senso di soggetto cui l'ordinamento riconosce il potere di escludere altri dall'accesso o dall'uso) ed accesso o uso del sistema non autorizzato, nonché a tutela dei delicati interessi posti in gioco, si è prevista la perseguibilità del reato a querela della persona offesa (art. 615-*ter* cod. pen.).

Non agevole appare poi individuare la persona offesa, l'unica titolare del diritto di querela. Essa non va confusa con eventuali altri soggetti che dalla realizzazione del fatto di reato subiscano soltanto un « danno », legittimante non la presentazione della querela, ma (eventualmente) la costituzione di parte civile.

Nulla esclude naturalmente che di fatto nella stessa persona vengano a coincidere sia la qualità sia di persona offesa, sia di danneggiato.

Ma resta il fatto che il reato è perseguito soltanto laddove sussista la querela della persona offesa, ovvero della persona il cui interesse è protetto dalla norma. Difficile dire in quale soggetto essa si identifichi, se cioè si tratti del titolare del sistema informatico (o che comunque ne dispone formalmente o ha diritto di escluderne l'accesso o l'uso a terzi), sulla falsariga della interpretazione data dalla dottrina al par. 202a StGB in tema di « sabotaggio informatico »[82], oppure del soggetto cui afferiscono le informazioni. La collocazione della disposizione nella sezione dei delitti contro la inviolabilità del domicilio sembra suggerire la prima soluzione[83].

---

[82] L. PICOTTI, *Studi di diritto penale dell'informatica*, cit., 76 s.

[83] Sul rapporto tra diritto di querela e persona offesa cfr. F. GIUNTA, *Interessi privati e deflazione penale nell'uso della querela*, Milano, 1993.

Il comma 2 dell'art. 615-*ter* cod. pen. contempla tre ipotesi aggravate punite con la reclusione da uno a cinque anni.

Le prime due non presentano difficoltà particolari. Si tratta, nell'un caso, del fatto commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, o da chi esercita anche abusivamente la professione di investigatore privato (comma 2, n. 1); nell'altro, dell'ipotesi in cui il colpevole, per commettere il fatto, usi violenza sulle cose o alle persone, ovvero sia palesemente armato (comma 2, n. 2).

A quest'ultimo proposito ricordiamo che la stessa legge n. 547/1993 (art. 1) ha integrato il concetto di *violenza sulle cose*, aggiungendo un terzo comma all'art. 392 cod. pen. nell'ambito della disciplina sull'esercizio arbitrario delle proprie ragioni.

La nuova disposizione riconduce all'alveo della violenza sulle cose anche il caso in cui il programma informatico venga alterato, modificato o cancellato in tutto o in parte, ovvero l'ipotesi in cui venga impedito il funzionamento di un sistema informatico o telematico.

Si tratta di una di quelle definizioni che, pur non essendo inserite tra i principi generali del Codice Penale, tuttavia hanno portata trascendente la disposizione stessa, in quanto al loro contenuto deve farsi rinvio ogni qual volta altre norme (del Codice Penale o di leggi speciali) richiamino il concetto di violenza sulle cose.

La dottrina, ad esempio, ritiene che anche la violenza sulle cose possa rientrare fra le modalità di realizzazione della violenza privata *ex* art. 610 cod. pen.[84].

La stessa efficacia generale è sottesa dal comma 4 dell'art. 307 cod. pen., ove si definisce il concetto di prossimi congiunti « agli effetti della legge penale » (ed in ciò appare inequivoca la volontà legislativa di esprimere un concetto di portata generale che fuoriesce dagli angusti limiti del delitto contro la personalità dello Stato, nella cui disciplina la specificazione si inserisce).

Proprio tale peculiarità appare significativa anche in relazione al comma 3 dell'art. 392 cod. pen., poiché la definizione, a differenza di altre, pure contemplate dalla legge n. 547/1993 (ad esempio, la descrizione del « documento informatico » *ex* artt. 491-*bis* e 621 cod. pen., ovvero quella di « corrispondenza » ai sensi dell'art. 616 cod. pen.), vale non solo nel contesto del delitto di esercizio arbitrario delle proprie ragioni o, semmai, nell'ambito di una determinata sezione o capo del Codice Penale, ma anche in ordine ad ogni norma che richiami il concetto di « violenza sulle cose » (ad esempio, l'art. 625, n. 2 cod. pen. prevede una circostanza aggravante speciale per il furto, se questo è stato commesso con *violenza sulle cose*).

Invece, la tecnica della definizione di concetto a livello di singole disposizioni o di singoli capi o sezioni del codice, diversamente dall'orientamento palesato dai codificatori che hanno optato per definizioni valide per l'intero ordinamento penale (sebbene non necessariamente inserite nella parte generale del codice), o quanto meno per il codice stesso (si pensi alla citata nozione di « prossimi congiunti » contemplato dall'art. 307, comma 4, cod. pen. italiano o alla terminologia definita dai parr. 11 e

---

[84] M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, 1994, 12 ss.

12 cod. pen. tedesco), non appare nuova, se si ricorda il par. 202a StGB in tema di spionaggio di dati, che al comma 2 appunto offre una definizione di « dato informatico » efficace ai soli sensi del comma 1 della medesima disposizione.

L'ultima ipotesi (n. 3) descritta dal comma 2 dell'art. 615-*ter* cod. pen. riguarda il caso in cui dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Come nella analoga ipotesi contenuta nell'art. 420 cod. pen., il legislatore si è voluto cautelare prevedendo una ipotesi di reato qualificato dall'evento per il caso in cui la distruzione o il danneggiamento del sistema sia conseguenza non voluta della condotta prodromica di accesso abusivo dell'agente[85].

Satelliti del reato base di abuso ed uso non autorizzato del sistema informatico e telematico sono altre fattispecie previste rispettivamente dagli artt. 615-*quater* e 615-*quinquies* cod. pen.

La prima punisce (con la reclusione sino ad un anno e con la multa sino a dieci milioni) chi, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Si tratta di una sorta di diffusione di notizie riservate, caratterizzata dal dolo specifico, ovvero al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Deve anche essere presente un requisito di antigiuridicità speciale, descritto in termini di « abusivamente »[86].

Singolare appare invece il disposto dell'art. 615-*quinquies* cod. pen., incentrato sulla diffusione, comunicazione o consegna di un programma informatico avente *per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati e dei programmi ad esso pertinenti, ov-*

---

[85] Per le brevi considerazioni svolte su questo punto si veda *supra* par. 4.

I fatti incriminati aventi ad oggetto sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico comportano l'applicazione di limiti edittali di pena più elevati, ovvero della reclusione da uno a cinque anni (se si tratta della fattispecie base di cui al comma 1) e da tre a otto anni (se il fatto integra gli estremi di una delle circostanze aggravanti previste dal comma 2).

Sul punto osserviamo che, a prescindere dalla lodevole intenzione di circondare di maggiore tutela i sistemi informatici di « interesse pubblico », il dettato normativo appare carente sotto il profilo della tassatività. La espressione « comunque di interesse pubblico » è troppo generica e rende elastici i limiti di applicabilità dell'aumento di pena: infatti i collegamenti tra sistemi di elaborazione informatica e soprattutto telematica costruiscono una rete inestricabile, nella quale profili di interesse pubblico rappresentano una eventualità non remota, ma difficile da circoscrivere. Tutte le ipotesi aggravate rendono il reato perseguibile d'ufficio e lo assoggettano alla competenza del Tribunale (art. 6 cod. proc. pen.).

[86] La pena è aggravata se ricorre taluna delle circostanze di cui ai nn. 1 e 2 del comma 4 dell'art. 617-*quater* cod. pen., sulla quale torneremo in prosieguo. La competenza è pretorile anche nella fattispecie aggravata ed il reato è procedibile d'ufficio: a riguardo si è ritenuto che l'approntamento di sistemi di sicurezza da parte del titolare del sistema sia presupposto essenziale per la configurazione dell'illecito, per cui la violazione del sistema stesso rappresenta una lesione dell'interesse pubblico che esclude la rimessione dell'azione penale alla persona offesa.

vero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

La diffusione di programma « infetto » viene punita sia nel caso in cui il danneggiamento sia scopo della condotta, sia nell'ipotesi in cui ne sia la conseguenza[87]: la estensione della fattispecie appare quindi indeterminata e notevole, forse non sufficientemente giustificata dalla pericolosità già ricordata insita nelle tecnologie informatiche.

Inoltre va notato che abbiamo di fronte una fattispecie cui sta stretta la collocazione nell'ambito dei delitti contro l'inviolabilità del domicilio e che forse avrebbe trovato più consona allocazione nell'ambito dei delitti contro il patrimonio, trattandosi pur sempre di una condotta criminosa strettamente connessa alla integrità del « patrimonio » informatico, più che alla libertà personale del titolare del sistema.

8. *(segue)* b) LE INTERPOLAZIONI NELLE COMUNICAZIONI INFORMATICHE O TELEMATICHE.

Tra i delitti di « indiscrezione »[88] vanno di certo annoverate le ipotesi incentrate sulla violazione dei segreti.

Il legislatore (art. 8, legge n. 547/1993), a fronte della obsolescenza dei sistemi di trasmissione delle informazioni ed al progresso della tecnologia, si è cautelato precisando che le norme contenute nella sezione (V), concernente i delitti contro la inviolabilità dei segreti (nel capo III - Delitti contro la libertà individuale del Titolo XII - Delitti contro la persona), norme relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, « si applicano a qualunque altra trasmissione a distanza di suoni, immagini o altri dati » (art. 6230-*bis* cod. pen.).

La disposizione sostituisce il dettato introdotto dall'art. 4 della legge n. 98/1974, che si limitava a rendere operante la fattispecie in relazione a « qualunque altra trasmissione di suoni, immagini o altri dati effettuata con collegamento su filo od onde guidate ».

1) Il concetto di corrispondenza (art. 616 cod.pen.).

Nel contesto testé ricordato si colloca la nuova definizione di « corrispondenza », estesa a quella « informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza » (art. 616 cod. pen., ultimo comma, sostituito dall'art. 5, legge n. 547/1993).

L'integrazione dell'art. 5 vale agli effetti della (sola) sezione in cui l'art. 616 cod. pen. è ospitato, ovvero nell'ambito dei delitti contro l'inviolabilità dei segreti[89].

La nozione di corrispondenza *ex* art. 616 cod. pen. non è efficace per tutte le altre ipotesi in cui viene in considerazione il concetto di « corrispondenza », per cui non vale, ad esempio, nell'ambito del d.P.R. n.

[87] A. ROSSI VANNINI, *La criminalità informatica*, cit., 450 s.

[88] MAURACH - SCHRÖDER - MAINWALD, *Strafrecht-Besonderer Teil*, cit., 255 s.

[89] A. ROSSI VANNINI, *La criminalità informatica*, cit., 447 ss.

431/1976 (artt. 36 e 37) contenente disposizioni relative all'ordinamento penitenziario e alle misure privative della libertà.

2) Le intercettazioni di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi (artt. 617-quater, -quinquies, -sexies *cod. pen.; artt. 266*-bis *e 268 cod. pen.).*

La legge n. 547/1993 si è anche preoccupata di adeguare la normativa italiana alla Raccomandazione n. R (89) 9 del Comitato dei Ministri dell'Unione Europea, che include l'intercettazione informatica nell'elenco minimo dei reati da prevedere nel quadro di una politica criminale relativa alla legislazione sulla criminalità informatica.

In tal senso il tessuto del codice è stato arricchito di tre nuove fattispecie che sanzionano le condotte criminose di intercettazione delle comunicazioni informatiche.

Le norme riguardano comportamenti che fino ad ora sono stati puniti soltanto in relazione alle comunicazioni o conversazioni telefoniche o telegrafiche[90].

Nel 1993 il legislatore ha ritenuto opportuno non limitarsi a sostituire il dettato di tali disposizioni con precetti relativi anche alle comunicazioni informatiche o telematiche, ma introdurre nel Codice Penale nuove fattispecie « parallele » incriminanti rispettivamente la intercettazione, impedimento o interruzione illecita di comunicazioni informatiche (art. 617-*quater* cod. pen.), la installazione di apparecchiature atte ad intercettare, impedire od interrompere dette comunicazioni (art. 617-*quinquies* cod. pen.), nonché la falsificazione, alterazione o soppressione del contenuto di dette comunicazioni (art. 617-*sexies* cod. pen.).

Come notato, la struttura della nuova fattispecie non si discosta da quella delle ipotesi introdotte dalla legge n. 98/1974.

L'art. 617-*quater* cod. pen. prevede la pena della reclusione da sei mesi a quattro anni per la intercettazione (ovvero presa di cognizione), nonché l'interruzione o impedimento delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi: l'espressione abbraccia uno spettro così ampio di ipotesi da risultare del tutto indeterminato.

La condotta deve essere « fraudolenta ».

Parimenti punita, ma solo in via sussidiaria (cioè « salvo che il fatto costituisca più grave reato »), è la condotta di rivelare, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle sopradette comunicazioni[91] (art. 617-*quater*, comma 2, cod. pen.).

---

[90] Infatti, a seguito della riforma operata dalla legge 8 aprile 1974, n. 98, si è sanzionata non solo la cognizione, interruzione o impedimento illecito di comunicazioni telegrafiche o telefoniche (art. 617 cod. pen.), ma anche la installazione di apparecchiature atte ad intercettare o impedire dette comunicazioni o conversazioni (art. 617-*bis* cod. pen.) e la falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-*ter* cod. pen.).

[91] Ipotesi aggravate (punibili con la reclusione da uno a cinque anni) sono previste dal comma 4 del medesimo art. 617-*quater* cod. pen., ricorrenti se il fatto è commesso 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero

Incriminata è anche la condotta prodromica alla effettiva intercettazione, impedimento o interruzione delle comunicazioni, consistente nella mera installazione di apparecchiature atte a tal fine, sempre che ciò non sia consentito dalla legge (art. 617-*quinquies* cod. pen.).

Questa costituisce una evidente forma di anticipazione della soglia della punibilità, connotata dalla particolare severità della sanzione, presumibilmente motivata dalla potenziale pericolosità del comportamento dell'agente: notiamo, infatti, che il minimo edittale di pena per la mera installazione di apparecchiature atte alla intercettazione, impedimento o interruzione delle comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi (art. 617-*quinquies* cod. pen.), è più elevato del limite edittale minimo previsto per la effettiva intercettazione, impedimento o interruzione di essi[92] (art. 617-*quater* cod. pen.).

Con l'art. 617-*sexies* cod. pen. si punisce (da uno a quattro anni) la falsità in comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

La struttura dell'illecito è la medesima del delitto *ex* art. 617-*ter* cod. pen. a proposito delle comunicazioni telegrafiche o telefoniche.

Gli elementi dell'illecito richiamano in parte la fattispecie di falsità in scrittura privata di cui all'art. 485 cod. pen.[93]

Identico il dolo specifico, consistente nel fine di recare a sé o ad altri un vantaggio o di arrecare ad altri un danno.

Elemento costitutivo del reato è anche l'uso o il lasciare che altri faccia uso della comunicazione falsa o alterata.

La condotta consiste nel « formare falsamente » o nell'« alterare o sopprimere, in tutto o in parte, il contenuto anche occasionalmente intercettato »[94].

Le condotte punite dagli artt. 617-*quater* e -*quinquies* cod. pen. devono essere « illecite », ovvero poste in essere oltre i limiti di eventuali autorizzazioni specifiche che, in via derogatoria ed assolutamente eccezionale, consentano restrizioni — generalmente vietate — del diritto alla riservatezza. Lo impone espressamente l'art. 617-*quater* cod. pen., inserendo il termine « illecito » nel dettato della disposizione; lo si inferisce dalla clausola « fuori da i casi consentiti dalla legge », contenuta nell'art. 617-*quinquies* cod. pen.

---

con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato. Le circostanze di cui ai nn. 2 e 3 coincidono con quelle previste dal n. 1 dell'art. 615-*ter*, comma 2, cod. pen. e denotano la particolare gravità della condotta del soggetto qualificato che approfitta delle prerogative garantitegli dalla propria posizione per utilizzare le informazioni contenute nel sistema informatico o telematico oltre i limiti consentitigli. Il delitto di cui all'art. 617-*quater* cod. pen. è perseguibile a querela della persona offesa nella fattispecie di base, di competenza pretorile; d'ufficio, nelle ipotesi aggravate (comma 3), per le quali è competente il Tribunale.

[92] Si applicano le medesime circostanze previste dall'art. 617-*quater*, comma 4, cod. pen. (art. 617-*quinquies*, comma 2, cod. pen.). Anche in tal caso la competenza appartiene al Pretore per l'ipotesi base, al Tribunale per quelle aggravate. Il delitto è comunque perseguibile d'ufficio.

[93] A riguardo da ultimo cfr. A. NAPPI, *I delitti contro la fede pubblica*, *in Giurisprudenza sistematica di diritto penale. Codice penale. Parte speciale*, V, Torino, 2ª ed., 1996, 163 ss.

[94] Trovano applicazione le circostanze previste dall'ultimo comma dell'art. 617-*quater* cod. pen. Per la perseguibilità penale e per la competenza valgono le osservazioni svolte a proposito dell'art. 617-*quinquies* cod. pen.

Significativa in tal senso l'estensione alle comunicazioni informatiche e telematiche della disciplina delle intercettazioni legittimate dal Codice di Procedura Penale.

L'art. 11 della legge n. 547/1993, infatti, introducendo l'art. 266-*bis* cod. proc. pen., consente le intercettazioni di comunicazioni relative a sistemi informatici o telematici ovvero intercorrenti tra più sistemi nei procedimenti relativi ai reati indicati nell'art. 266 cod. proc. pen. (che già legittimava le intercettazioni di conversazioni o comunicazioni telefoniche e « di altre forme di telecomunicazione » nei procedimenti per delitti connotati da una particolare gravità), nonché *ai reati commessi mediante l'impiego di tecnologie informatiche o telematiche*.

Quest'ultima espressione va evidenziata perché permette di ampliare enormemente la sfera di liceità delle intercettazioni, non più circoscritta ai procedimenti concernenti particolari tipologie di reati, ma estesa ai procedimenti relativi ad *ogni ipotesi di reato, purché commesso con l'impiego di tecnologie informatiche o telematiche*.

Appare evidente che per legittimare dette intercettazioni sarà sufficiente che un reato, qualunque esso sia, sia stato commesso o comunque agevolato, ad esempio, dalla tenuta di una banca dati, per cui anche il semplice furto continuato, realizzato attraverso più condotte poste in essere ai danni di diversi esercizi pubblici, consentirà le intercettazioni, se l'agente, ad esempio, abbia conservato i dati relativi a detti esercizi pubblici o al suo « disegno » in un programma di memoria.

Consequenziale all'inserimento dell'art. 266-*bis* cod. pen. è la modifica dell'art. 268 cod. proc. pen., contenente le garanzie relative alla esecuzione delle intercettazioni.

La norma è stata opportunamente adeguata per consentire l'esercizio del diritto di difesa qualora le intercettazioni vengano poste in essere ed entrino a far parte dei mezzi di ricerca dalla prova.

3) La rivelazione del contenuto di documenti segreti (art. 621 cod.pen.).

La integrazione dell'art. 621 cod. pen. in tema di rivelazione di documenti segreti ad opera dell'art. 7 della legge n. 547/1993 è altresì rilevante, poiché definisce il concetto di documento, sebbene ai limitati fini della applicazione della disposizione stessa.

Torneremo sul punto nel paragrafo successivo. Sia sufficiente per ora segnalare soltanto che l'art. 621, comma 1, cod. pen. punisce (con la pena alternativa della reclusione fino a tre anni o con la multa da lire duecentomila a due milioni) la condotta di chiunque, il quale, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, da altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela senza giusta causa ovvero lo impiega a proprio o altrui profitto, se dal fatto deriva nocumento.

La novella chiarisce, introducendo un nuovo comma nell'art. 621 cod. pen., fra il primo ed il comma 3[95] che, agli effetti della disposizione di

[95] Quest'ultimo prevede la perseguibilità a querela del reato, di competenza pretorile.

cui al comma 1, è considerato *documento* anche qualunque supporto informatico contenente dati, informazioni o programmi.

La definizione — lo si sottolinea fin da ora — trova due limiti di fondo: in primo luogo, appare estremamente generica — poiché richiede il ricorso ai parametri individuati dalla giurisprudenza —, non essendo fissato alcun requisito specifico se non il rapporto di incorporazione (del documento) in un « supporto » informatico (non solo materiale, quale ad es. un *floppy disk*, ma anche un *byte*); la nozione di documento, inoltre, vale ai fini della individuazione del contenuto del solo art. 621 cod. pen., con eslcusione di qualunque altra norma nella quale ricorra detto concetto.

Una concezione di documento informatico, pertanto, settoriale e decisamente parziale.

Qualche elemento in più, come si dirà nel paragrafo successivo, compare nella definizione di documento inserito nel Codice Penale ai fini della applicazione delle fattispecie in tema di falsità in atti (art. 491-*bis* cod. pen.).

9. Il concetto di « documento informatico » e le relative ipotesi di falsità.

Si è anticipato che la legge del 1993 non ha inteso introdurre un concetto omnicomprensivo di documento informatico, ma si è accontentata di fornire alcuni fotogrammi di esso, come riguardando il concetto di documento da angolature diverse.

La questione appare di indiscutibile rilevanza, posto che la maggior parte delle operazioni finanziarie e commerciali si svolge attualmente attraverso la gestione di dati informatici[96]. Il concetto di « documento », quindi, diviene determinante per assicurare la certezza dei traffici giuridici.

L'art. 491-*bis* cod. pen. descrive il documento informatico nell'ambito delle falsità documentali e stabilisce che, se taluna delle falsità previste dal capo III (relativo appunto alla falsità in atti) concerne un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per « documento informatico » si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destianti ad elaborarli.

La definizione si rivela interessante sotto diversi punti di vista.

Innanzi tutto per la prima volta si introduce nel Codice Penale un concetto di documento il cui contenuto, anche in relazione ai documenti cartacei tradizionali, era rimessa fino ad oggi alla interpretazione giurisprudenziale[97].

[96] Sulla facilità di alterazione delle informazioni prima che esse vengano incorpoate in « documenti » cfr. L. Picotti, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir. inf.*, 1985, 958 ss.; circa la difficoltà di applicare a normativa in tema di falsificazione documentale cfr. L. Picotti, *Studi di diritto penale dell'informatica*, cit., 59 ss.

[97] Per una ricostruzione del dibattito in materia cfr. A. Nappi, voce *Fede pubblica*, in *Enc. giur. Treccani*, Roma, XIV, 1989, 2 ss. Id., *Falso e legge penale*, Milano, 37 ss.; S. Patti, voce *Documento*, in *Dig. disc. pen.*, VII, 1991, 3 s. A differenza della soluzione italiana, il Codice Penale tedesco rinuncia ad una descrizione della natura dell'oggetto materiale della falsificazione: L. Picotti, *Studi sul diritto penale dell'informatica*, cit., 60 ss., che ha approfondito in particolare anche lo studio delle conseguenze della scelta a favore del-

La accezione codificata in effetti recepisce le caratteristiche enucleate dalla giurisprudenza per descrivere il concetto di documento ai fini dei reati di falsità documentale, ovvero: contenuto di pensiero; efficacia probatoria; supporto esteriore[98].

Una sola peculiarità, invece, pur evidenziata dalla giurisprudenza in relazione al documento informatico, non è stata recepita dal testo legislativo. Si tratta del requisito della provenienza, della paternità del documento stesso, requisito sul quale la legge ha ritenuto di soprassedere, forse anche per la difficoltà di individuazione.

Chi sia il titolare di tale posizione, infatti, appare problematico. Potrebbe trattarsi, ad esempio, di colui che ha la detenzione della banca dati; ovvero, di chi ha inserito nell'elaboratore l'informazione; ovvero di chi l'ha trasformata in documento, attraverso la traduzione dell'informazione in supporto visibile; o ancora di chi ha ideato il programma.

Le incertezze sul punto sono molteplici ed incidono anche sulla determinazione del carattere pubblico e privato del documento, con prevedibili difficoltà di individuazione della norma applicabile[99].

Sembra potersi affermare che la « pubblicità » del documento vada inferita dalla natura del soggetto che è detentore dell'archivio, che di esso è il referente. Ma naturalmente in tal modo non si fa altro che spostare i termini del problema senza pervenire ad una soluzione del medesimo. La questione diventa allora l'individuazione del soggetto che può fregiarsi della qualifica di « referente » dell'archivio.

Infine, non di poco conto è l'applicazione settoriale della definizione che, essendo limitata al capo delle falsità in atti contenuta nel Codice Penale, esclude la applicazione della fattispecie ad altri fini, ad esempio in ordine alle falsità contenute in branche della legislazione speciale, come in quella tributaria.

10. Il diritto penale delle carte di credito.

Con l'entrata in vigore dell'art. 12 della legge 5 luglio 1991, n. 197, contenente « provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio », si sono introdotte nell'ordinamento penale nuove fattispecie volte a punire specificamente alcune condotte aventi ad oggetto le carte di pagamento.

La necessità della introduzione della normativa risiede, al solito, nella inadeguatezza delle norme esistenti prima della emanazione della disciplina in esame.

---

la tutela dell'affidamento del valore probatori dei dati informatici (parr. 270-274 e 348 StGB).

[98] Nell'ordinamento francese la fattispecie di falso informatico, pur essendo stata prevista nel testo originario della legge n. 88-19 del 5 gennaio 1988 (art. 462-5 cod. pén.: sul punto cfr. D. Fondaroli, *I problemi della criminalità informatica e la legge francese n. 88-19 del 5 gennaio 1988*, cit., 799 *s*), nel vigente Codice Penale francese è assorbita dalla definizione generale di « falsità » (art. 441-1 cod. pén.), intesa come « ogni alterazione fraudolenta della verità, tale da cagionare un danno e compiuta attraverso qualsiasi mezo, in uno scritto o in un altro supporto dell'espressione del pensiero, che abbia per oggetto o che possa essere efficace a fondare, un diritto o un fatto avente conseguenze giuridiche ».

[99] Sul punto cfr. A. Merli, *Il falso nei documenti informatic*m in *Giust. pen.*, 1995, 189 ss.

Per comprendere l'entità del fenomeno occorre ricordare che gli abusi della carta di credito o di pagamento possono essere posti in essere sia dal titolare della carta di credito, quando egli utilizzi la carta oltre i limiti consentitigli; sia da un soggetto estraneo, che si serva della carta di pagamento altrui.

Nessun problema si è posto finché la condotta ha per oggetto il supporto materiale nel quale la carta si sostanzia: in tal caso l'« estraneo », che di essa si avvale, potrà essere perseguito, ricorrendone i presupposti, per furto, per appropriazione indebita o quant'altro.

La questione si pone, invece, in relazione alle condotte incentrate sull'uso non autorizzato della carta, ovvero al di fuori ed al di là del mero e prodromico fatto della eventuale sottrazione della carta[100].

L'applicazione della normativa previgente poneva serie difficoltà: quanto alla operatività della truffa, si diceva che non potesse configurarsi il requisito della induzione in errore di « taluno ». Circa l'applicabilità del furto, si è obiettato che la consegna delle cose appare volontaria, in quanto il soggetto che digita appare allo sportello erogatore come formalmente legittimato al prelievo, col che viene meno l'elemento dell'impossessamento e/o spossessamento del bene contro la volontà del proprietario, tipico del delitto di furto. Né miglior fortuna vanta la tesi della appropriazione indebita[101].

In Francia il prelievo di danaro dal Bancomat, da parte del titolare della carta, oltre il limite convenuto, è stato qualificato dalla giurisprudenza come illecito contrattuale, derivante dalla violazione della provvista stabilita al momento della conclusione del contratto tra banca e cliente[102].

A fronte di tale situazione si è ritenuta opportuna la elaborazione di una disciplina *ad hoc*.

L'art. 12 della legge n. 197/1991 sanziona (con la reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni) condotte differenziate, in particolare l'indebita utilizzazione della carta di credito (si punisce il comportamento del soggetto, non titolare della carta che, al fine di trarne profitto per sé o per altri, indebitamente utilizza carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi); la falsificazione o alterazione della medesima (ovvero la condotta di chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di

[100] Per una approfondita panoramica sul punto cfr. Cour. Cass. 4 novembre 1983, in questa *Rivista*, 1985, 720 ss., con nota di G. Corrias Lucente, *Informatica e diritto penale*, cit., 726 ss.

[101] Sui vari orientamenti a riguardo in relazione ai diversi ordinamenti cfr. L. Tria, *Osservazioni in tema di « reati elettronici »*, in *Arch. pen.*, 1984, 283 ss.; K. Tiedemann, *Criminalità da* computer, in *Pol. dir.*, 1984, 626 ss.; G. Corrias Lucente, *Bancomat e rilevanza penale dell'abuso da parte del correntista*, in questa *Rivista*, 1985, 720 ss.; A. Alessandri, *Criminalità organizzata*, in *Riv. trim. dir. pen. econ.*, 1990, 655 s.; D. Fondaroli, *Criminalità inforamtica e normativa penale italiana: cerchi intersecantesi oppure cerchi esterni l'uno all'altro?*, in L. Sola - D. Fondaroli, *A proposito della criminalità informatica*, cit., 56 ss.

[102] G. Corrias Lucente, *Bancomat e rilevanza penale dell'abuso da parte del correntista*, cit., 720; per il profilo comparatistico si veda C. Pecorella, *L'abuso di distributori automatici di banconote*, in *Riv. it. dir. proc. pen.*, 1990, 651.

servizi); infine, il possesso, la cessione o l'acquisizione di tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento con essi prodotti[103].

La disposizione si ripropone quindi di sottoporre al medesimo trattamento sanzionatorio diverse tipologie di condotta, che spaziano dalla falsificazione o alterazione della carta, alla condotta prodromica di possesso di carta di illecita provenienza, all'utilizzo della carta altrui, al trasferimento della carta di illecita provenienza.

La condotta di « utilizzazione » della carta altrui presuppone sì la non titolarità della carta stessa, ma non la illecita provenienza della medesima. Quest'ultima ipotesi, invece, insieme all'« abuso » di carta sottratta al legittimo titolare, è invece riconducibile alla diversa fattispecie di « possesso » di carta di credito o di pagamento di illecita provenienza[104].

L'« abuso » della carta, perciò, consiste nell'impiego della carta altrui, lecitamente posseduta. In tal senso è l'uso ad essere indebito, ovvero non consentito secondo la legge extrapenale.

Al momento della realizzazione della condotta deve essere presente nell'agente il dolo specifico del fine di profitto per sé o per altri[105].

Anche in ordine alla falsificazione della carta di credito o di pagamento si è prevista una anticipazione della soglia di punibilità, essendo sufficiente per l'integrazione del reato la mera falsificazione della carta, a prescindere dall'uso della stessa.

Il tenore della norma non esclude che la falsificazione possa essere ascritta anche al titolare della carta.

La condotta si estrinseca in una contraffazione della carta, mentre è richiesto il dolo specifico del profitto.

Infine la condotta di possesso, cessione e acquisizione di carta di credito presuppone la provenienza della stessa da un precedente illecito, anche civile o amministrativo: l'illecito civile può verificarsi, ad esempio, quando il soggetto, che si era impegnato alla restituzione della carta, non adempia l'obbligo ma ceda la carta ad un terzo pur non essendo più legittimato.

La cessione presuppone la disponibilità della carta, ed insieme alla alienazione concerne la problematica del trasferimento della carta stessa.

Anche in tal enso il dolo specifico consiste nel fine di profitto per sé o per altri.

---

[103] A commento di tale normativa si legga C. Pecorella, *Il nuovo diritto penale delle carte di pagamento*, in *Riv. it. dir. proc. pen.*, 1993, 258 ss.; Id., *Commento all'art. 12, l.n. 157*, 1991, *Le nuove leggi civili commentate*, 1993, 1097 ss.

[104] C. Pecorella, *Il nuovo diritto penale delle carte di pagamento*, cit., 262.

[105] Si è notato a riguardo che « l'apparente profitto del quale è fatto calcolo, in ultima analisi si risolve sul piano dell'offesa », poiché il fine qualifica l'indebito utilizzo, la falsificazione, ecc. della carta di credito o di pagamento, considerato in una prospettiva di « abuso della sua propria funzione economico-patrimoniale »: G. Azzali, *Scritti di teoria generale del reato*, Milano, 1995, 184).