Roberto Caso, *Criminalità informatica: «bombe logiche» e danneggiamento di software* (Nota a A. Torino, 29 novembre 1990), in *Foro it.*, 1991, II, 228

Criminalità informatica: 'bombe logiche' e danneggiamento di software.

I. - Con la sentenza in epigrafe sembra volgere al termine una delle prime vicende giudiziarie relative al sabotaggio del software commesso con l'uso del computer (la pronuncia parzialmente riformata è Pret. Torino 23 ottobre 1989, Foro it., 1990, II, 462, con osservazioni di R. CASO, Sabotaggio del «software» e reato di danneggiamento, ivi riferimenti giurisprudenziali e dottrinali).

La corte, pur dichiarando il proscioglimento degli imputati dal reato di danneggiamento ex art. 635 c.p. per la sopravvenuta (e tanto agognata!) amnistia, ha confermato in toto le argomentazioni svolte nella sentenza pretorile e, con esse, la condanna degli stessi imputati al risarcimento dei danni e alla rifusione delle spese giudiziali (in primo grado era stata accordata una provvisionale di non lieve entità: 20.000.000 di lire).

I rari interventi, quale quello odierno, di una giurisprudenza nostrana ancora pionieristica offrono parsimoniose occasioni per accostarsi più da presso al tema della c.d. Computerkriminalität (come è facilmente intuibile, la materia segue la frenetica espansione dell'universo informatico, ciò che rende non agevole, e forse poco indicato, lo studio monografico di ampio respiro; in Italia, comunque, esso si limita al testo di CORRERA-MARTUCCI, I reati commessi con l'uso del computer, Padova, 1986). Per tale motivo, come già facemmo in altra occasione (con alcune guide-lines sullo studio della criminalità da computer), ci soffermeremo, prima di riesaminare l'argomento che ci coinvolge più da vicino (id est, il sabotaggio del software), su qualche approfondimento e aggiornamento di ordine generale sui computer crimes, facendo tesoro di alcune sollecitazioni comparatistiche.

II. - Nel nostro paese, una seria riflessione – comunque ancora esigua sul versante della dottrina giuridica – sembra gradualmente sostituire un approccio confuso e disorientato al problema del «crimine informatico».

Alcune colossali frodi a danno delle reti bancarie informatizzate, infiltrazioni, tanto spettacolari quanto pericolose, in alcuni sistemi di difesa nazionali e, per ultimo, il diffondersi dei c.d. virus informatici hanno suscitato clamore ed allarme sociale (qualche eclatante episodio, dei tanti che dagli onori della cronaca rifluiscono nelle trattazioni giuridiche sul tema, si può rinvenire in CASO, op. cit., 463; qui basti aggiungere due recenti casi: il primo dai toni grotteschi, che evocano i ricatti fumettistici del cattivo di turno, è riportato dal Corriere della Sera del 29 novembre 1990 e riguarda un virus denominato «aids», diffuso dal suo ideatore spedendo dischetti «infetti», che una volta inseriti nell'elaboratore comunicavano all'utente l'alternativa se pagare per l'antidoto o subire gli effetti del virus; il secondo, anch'esso curioso oltre che inquietante, riguarda la penetrazione, per mezzo di una banale strumentazione telematica, nei sistemi informatizzati di un centro di sperimentazioni nucleari d'oltralpe, effettuata da giornalisti di un quotidiano francese al solo scopo di dimostrare la vulnerabilità di tali apparecchiature computerizzate: cfr., in merito, AA.VV., Droit de l'informatique (informatique, télématique, réseaux), ed. Lamy, 1991, 1453).

Si tratta di proverbiali punte di iceberg rispetto ad un fenomeno allargato, il cui sviluppo è legato alla progressione geometrica dell'utenza informatica ed alla naturale vulnerability to crime degli elaboratori elettronici; fenomeno della cui entità solo ora si inizia a prendere coscienza (le prime stime ci forniscono dati men che confortanti, con una crescente percentuale dei danni causati da comportamenti intenzionali a fronte di quella riguardante gli incidenti casuali, v., ad es., le cifre riportate da Il Sole 24 Ore del 5 novembre 1990; eguale tendenza connotano le statisiche statunitensi sui danni arrecati dai computer crimes, v., in merito, CHEN, Computer crime and the computer Fraud and Abuse Act of 1986, in Computer law journal, 1990, 74, il quale, peraltro, dubita della precisione di questi rilievi, non fondati su una definizione univoca e sicura di computer crime).

Con tutta probabilità, però, questi primi bilanci non rendono ragione dell'effettiva dimensione della criminalità da computer, anche perché le vittime, in molti casi software houses e operatori finanziari, preferiscono non ricorrere alla denuncia (i costi di una cattiva pubblicità che faccia eco alla fragilità delle difese dei sistemi informatici colpiti sarebbero molto spesso notevolmente superiori agli eventuali risarcimenti: pare che, negli Stati uniti, solo l'un per cento dei delitti venga scoperto, e che a sua volta di questa sparuta minoranza solo il quattordici per cento venga alla luce grazie alle denunce e che soltanto uno su 22.000 computer criminals finisca in prigione; cfr., sul punto, CHEN, op. cit., 77. Inoltre, in Italia, innescare un lungo meccanismo processuale, in quasi totale assenza di una legislazione ad hoc e di una giurisprudenza formata, non dà la sicurezza di trovare giustizia; come se ciò non bastasse, la disomogeneità delle varie normative statali garantisce, in alcuni casi, l'impunità dei «pirati informatici e telematici» che agiscono su scala internazionale).

Dunque, una cosa è certa: «il crimine informatico paga» e, per di più, è facilmente reiterabile, perciò i danni che esso comporta, in termini monetari, sono generalmente ingenti (cfr., sul punto, TIEDMANN, Criminalità da computer, in Politica del diritto, 1984, 618, il quale sottolinea che «l'azione e gli effetti del reato sono normalmente distanziati [...] con difficoltà considerevolmente maggiori di scoprire il fatto stesso. A questo si aggiunga l'efficacia duratura della delinquenza da computer: se il fatto riesce per la prima volta, diviene spesso ''permanente'' [...]. Da tali considerazioni emerge che l'incidenza dei danni della criminalità da computer è tendenzialmente molto alta»; cfr. anche PICOTT, Problemi penalistici in tema di falsificazione dei dati informatici, in Dir. informazione e informatica, 1985, 943).

Ulteriore, diretta conseguenza è l'aumento esponenziale della spesa in protezioni di ogni genere, nonché in copertura assicurative idonee, se non altro, ad arginare il rischio di «attacchi elettronici» (è forse inutile rilevare che intorno a tali misure protettive si muove ormai un giro d'affari di grosse proporzioni; si tratta, oltre che della predisposizione di personale di sorveglianza, di «scudi» fisici e, per ciò che riguarda gli interventi ex post, di tecniche di recupero dati, anche delle barriere c.d. logiche, id. est di tipo informatico, prodotte dalle stesse software houses e sulle quali avremo modo di tornare in seguito. Sul tema cfr. TRAVERSI, Il diritto dell'informatica 2, 1990, che, tra l'altro, illustra la nuova figura dell'auditor – di cui si avvalgono le grandi imprese americane – che si occupa di predisporre le strategie di difesa dei dati e le attività di controllo sulle procedure di elaborazione automatica. Anche il ricorso all'assicurazione è in aumento; cfr., su ques'ultima tematica, S. TRAVERSO, Assicurazione e software, in Dir. informazione e informatica, 1987, 312 e CORRERA-MARTUCCI, op. cit., 50 e 170).

Intanto, sul fronte dell'investigazione si cerca di mettere a punto le nuove sezioni specializzate di polizia e di iniziare una cooperazione sul piano transnazionale (anche l'Italia si è dotata di queste strutture e nell'ottobre dell'anno passato si è tenuto a Roma un convegno fra le squadre investigative europee che lottano contro questo tipo di criminalità: ne dava notizia Il Sole 24 Ore del 9 novembre 1990).

Altresì meritevoli di attenzione risultano i profili criminologici. Solitamente viene descritta una tipologia del «criminale informatico» che spazia dal giovane (o giovanissimo) hacker, il quale ha appena abbandonato le convulse geometrie dei videogames per darsi al «grimaldello elettronico», fino all'esperto in trasferimenti elettronici di fondi senza scrupoli (questo ritratto si ritrova di frequente nelle trattazioni di ordine generale sul nostro argomento, soprattutto in quelle più risalenti, ed è stato felicemente riassunto nel motto «dai colletti bianchi ai pantaloncini corti»: così SPREUTELS, La responsabilità penale connessa ad abusi nell'applicazione dell'informatica, in Dir. informazione e informatica, 1985, 127).

Tuttavia, una tale descrizione non evidenzia nella giusta misura la più segnalata diffusione e multiformità dell'uso deviato dell'ordinatore (in questo senso, la fattispecie in rassegna potrebbe

divenire paradigmatica – v., sul punto specifico, CASO, op. cit., 466 –, infatti è probabile che i rapporti commerciali di fornitura informatica non abbiano sempre raggiunto un elevato grado di sviluppo contrattuale, in grado di gestire e proteggere l'apporto innovativo ed il conseguente sfruttamento economico del prodotto informatico. Come abbiamo già accennato in altra occasione, la protezione del know-how costituisce, prima di tutto sul piano civilistico, una preoccupazione pressante, soprattutto in un paese dove non esistono leggi specifiche, che può spingere a farsi giustizia da sé; per avere un'idea della complessità di un contratto di fornitura informatica, v. FORTUNATO, Tutela del software, contratti informatici e diritti delle parti, in Quadrimestre, 1990, 14. Su tutt'altro terreno, ma sempre a proposito della limitatezza del quadro criminologico di solito tracciato, v. lo studio dal titolo di per sé inquietante di PAGLIARO, Informatica e crimine organizzato, in Indice pen., 1990, 241, nel quale viene anche trattato il rovescio della medaglia costituito dall'uso del mezzo informatico per la lotta al crimine organizzato; altrove la criminalità da computer presenta, invece, connotazioni terroristiche come nel caso del gruppo eversivo tedesco del 'Chaos computer club', v. AA.VV., Droit de l'informatique, cit., 1453).

Veniamo ora al punctum dolens della copertura legislativa dei computer crimes.

Mette conto rilevare che il nostro legislatore è finora rimasto 'sordo all'intenzion' della dottrina (almeno quella dominante), la quale in ogni suo intervento sull'argomento non manca di sollecitare l'introduzione di nuove fattispecie criminose. Non vi sono dubbi sulla fondatezza di questa esigenza (manifestata peraltro, al di là dell'applicazione della norma sul danneggiamento al caso di specie, anche dall'estensore della sentenza in epigrafe).

Essa appare avallata dal fatto che sotto ogni cielo, o quasi, al bivio cruciale fra il recupero e/o maquillage delle normative esistenti e l'introduzione di nuove figure di reato, si sia imboccata la seconda strada (ciò non toglie che una tale scelta sia maturata in un certo travaglio dottrinale e giurisprudenziale: valgano per tutti due esempi: in primo luogo quello degli Stati uniti, sul quale si veda CORRIAS LUCENTE, Informatica e diritto penale: elementi di comparazione con il diritto statunitense, in Dir. informazione e informatica, 1987, 531, per ciò che riguarda la sterminata letteratura americana qui basti rinviare al già richiamato CHEN, op. cit., il quale, tra l'altro, avanza perplessità sull'idoneità della normativa d'oltreoceano a controllare la criminalità in parola; in secondo luogo, il caso della Germania, nella quale si è sviluppato un acceso dibattito circa l'opportunità dell'introduzione di una fattispecie autonoma di sabotaggio del software).

Quantunque sia questa la deriva transnazionale, prima di metter mano alla pur urgente riforma occorre meditare attentamente su quali siano i profili del fenomeno che effettivamente sfuggono, de iure condito, alle maglie repressive della legge e su come essi andranno regolamentati (al di là dei disegni di legge decaduti e di piccoli interventi settoriali come la l. 1° aprile 1981 n. 121 sul nuovo ordinamento dell'amministrazione della pubblica sicurezza – cfr. in merito TRAVERSI, op. cit., 223 – , si è avuto, recentemente, qualche segnale di movimento; è stata, infatti, preannunciata l'imminente presentazione di un disegno di legge governativo sui computer crimes; la notizia è riportata da Il Sole 24 Ore del 15 novembre 1990).

Nelle esperienze straniere non mancano, d'altro canto, i primi esempi di disfunzioni nei nuovi apparati normativi (è il caso della nuova disciplina francese – loi 88-19 del 5 gennaio 1988, che ha novellato il code penal e il cui testo è riportato in Dir. informazione e informatica, 1988, 645 – riguardo la quale è stato avanzato il dubbio di un accavallamento tra i nuovi art. 462-3 e 462-4 del code penal, riguardanti entrambi il tema del sabotaggio informatico (cfr., in merito, AA.VV., Droit de l'informatique, cit., 1514; inoltre, la scelta sistematica di creare un nuovo capo autonomo nel code penal è oggetto di critiche anche da parte di una voce dottrinale italiana: v. M. MANTOVANI, I reati informatici nella recente esperienza francese: l'uso e l'accesso abusivi, in Dir. informazione e informatica, 1990, 885; non pochi problemi sembra porre il Computer Fraud and Abuse Act statunitense, su cui cfr. CHEN, op. cit., 76 s.).

Non è questa, ovviamente, la sede per condurre un'analisi sistematica delle numerose forme di computer crimes e per misurarne la riconducibilità nell'alveo del nostro codice penale; sarà sufficiente evidenziare come esse pongano problemi complessi e fra loro molto differenti.

Di là dalle varie classificazioni, si possono individuare essenzialmente tre filoni: le violazioni della privacy, alcune fattispecie di riproduzione abusiva del software (sembra, però, che in questo caso le sanzioni penali funzionino solo da supporto alla tutela civilistica da copyright) e le c.d. manipolazioni informatiche, all'interno delle quali bisogna distinguere le frodi informatiche, reati contro la fede pubblica e altri abusi del computer (accesso e uso non autorizzato, sabotaggio del software e dell'hardware, ecc.). Questi ultimi rappresentano, forse, il terreno più difficile sul quale si affrontano le diverse voci dottrinali e le differenti opzioni di politica del diritto (sulle manipolazioni informatiche e per un proficuo, schematico raffronto della situazione legislativa e prelegislativa nei diversi quadranti europei, cfr. SINDEN, Computer misuse in Europe, in Computer & software, ed. Backer & Mackenzie, 1990, 286 s.; sui computer crimes in generale, v., per gli Stati uniti, NIMMER, The law of computer technology, Boston/New York, 1985, cap. 9, e MANDEL, Computers, data processing and law. Text and cases, St. Paul, 1984, 153 s.).

Solo a mo' di esempio possiamo prendere l'accesso e l'uso non autorizzati dell'electronic data processing (si badi, l'esempio non è preso a caso: è facile intuire come l'unauthorized access and use, mercé un intervento diretto sulla consolle o, forse più di frequente, attraverso collegamenti telematici, sia il punto di partenza per la commissione di svariati computer crimes, fra i quali, va da sé, il sabotaggio del software). Dando per scontato che le norme in vigore non siano sufficienti a reprimere l'intera gamma di tali comportamenti (occorre, però, dire che all'interno della dottrina italiana già si trovano opinioni differenti: più favorevole ad un radicale intervento innovativo è PELLEGRINI, Uso non autorizzato del computer. Limiti e prospettive della tutela penale, in Dir. informazione e informatica, 1987, 289; su posizioni diverse è MANTOVANI, op. cit.) e che si debbano creare nuove ipotesi di reato, bisognerà dapprima risolvere il dilemma se configurare, o non, una sorta di delitto-ostacolo, volto a scoraggiare atti (accesso non autorizzato) che costituiscono il prius necessario per la commissione di alcuni abusi del computer (la nuova norma francese demandata alla repressione dell'accesso non autorizzato si presenta appunto come un esempio di delit obstacle; senza voler entrare nel merito dell'argomento, qui basterà rinviare a MANTOVANI, op. cit., 888 s., che ritiene la logica,che sta a monte dell'opzione francese, non trasferibile nel nostro ordinamento; per una discrasia sul punto tra i progetti di legge inglese e scozzese, v. SINDEN, op. cit., 286 s.). Il tema della tutela contro l'uso e l'accesso non autorizzati offre anche un valido esempio per i problemi di tecnica sanzionatoria legati alla protezione penalistica dalle manipolazioni informatiche (per un primo scorcio di questo campo d'indagine si può attingere ancora a MANTOVANI, op. cit., 900 s.).

Quel che finora si è detto dovrebbe rappresentare un caveat sufficientemente persuasivo sui pericoli di un'opera di rinnovamento affrettata e/o che porti ad una superfetazione di norme incriminatrici, con conseguente (ed ulteriore) intasamento nel settore della giustizia penale (un monito in questo senso si rinviene in SISTO, Diritto penale dell'informatica e recupero dei modelli tradizionali, in Critica pen., 1985, fasc. 3, 28).

III. - Veniamo ora al tema del sabotaggio del software (con questa espressione intendiamo riferirci a qualsiasi condotta di alterazione e distruzione di dati informatici operata tramite istruzioni indirizzate in qualunque modo al calcolatore) e alla sentenza in epigrafe.

Come già accennato in apertura, essa ricalca sostanzialmente le argomentazioni, svolte nella pronuncia di primo grado, che avevano portato il Pretore di Torino (sent. 23 ottobre 1989, cit.) ad affermare l'applicabilità dell'art. 635 c.p. ad una fattispecie di distruzione e alterazione – operate tramite un intervento alla consolle, ossia a contatto diretto con l'elaboratore oggetto della condotta – di programmi per computer e di basi di dati registrati su supporti magnetici.

Avendo già avuto occasione di svolgere alcuni rilievi in ordine alla pronuncia pretorile, riteniamo opportuno soffermarci più approfonditamente sui 'vantaggi' che la rada giurisprudenza ha ravvisato nella norma sul danneggiamento (è bene ricordare che, oltre le due pronunce di cui si discute, Trib. Torino 12 dicembre 1983, Foro it., Rep. 1984, voce Danneggiamento, n. 5 e voce Esercizio arbitrario delle proprie ragioni, n. 10, aveva ritenuto integrati gli estremi della «violenza alle cose» nella cancellazione di un programma). In altri termini, si tratta di verificare se questo atteggiamento sia finalisticamente apprezzabile – perché teso a colmare un vuoto di giustizia dovuto alla lamentata assenza di norme specifiche – ma ermeneuticamente errato (come ritiene una parte della dottrina) o, piuttosto, abbia un fondamento teorico.

Diciamo subito che le conclusioni a cui sono giunti i giudici torinesi sembrano persuasive anche se è necessario chiarirne i presupposti.

Non sembra si possa mettere in discussione il fatto che una condotta di alterazione o cancellazione di dati informatici (intesi in senso lato e cioè comprendenti sia programmi digitati in qualsiasi forma di linguaggio sia basi di dati) memorizzati su supporti magnetici si concretizzi in una modificazione fisica dei supporti stessi (è bene ricordare che da un punto di vista tecnico il metodo di memorizzazione magnetica del dato informatico è quello più impiegato). A questa conclusione si arriva se ci si sofferma un momento sulla spiegazione tecnica del processo di memorizzazione dei dati informatici su supporti magnetici (per una prima illustrazione tecnica, cfr. la motivazione di Pret. Torino 23 ottobre 1989, cit.; per un testo specialistico, v. MAIOCCHI, Teoria e applicazione delle macchine calcolatrici, Milano, 1984, 317, il quale chiarisce che «le variazioni del campo magnetico indotte dagli impulsi elettrici in arrivo vengono memorizzate sul disco o sul nastro come variazioni dello stato di magnetizzazione del supporto»).

Una tale precisazione consente di superare le riserve di chi, contrario all'applicazione dell'art. 635 c.p., mostra in primo luogo di dubitare che tali condotte di alterazione magnetica integrino di per se stesse un danneggiamento o una manomissione del supporto materiale (v., in questo senso, PICOTTI, La rilevanza penale degli atti di «sabotaggio» ad impianti di elaborazione dati (nota a Trib. Firenze 27 gennaio 1986, Foro it., 1986, II, 359, con nota di RAPISARDA), in Dir. informazione e informatica, 1986, 969, ivi rilievi comparatistici sulle nuove norme tedesche in tema di sabotaggio del software; problemi analoghi ai nostri si sono posti in Francia per l'interpretazione dell'art. 434 code penal equivalente del nostro art. 635; cfr., in merito ad essi e per un commento ai nuovi art. 462-2, 462-3 e 462-4, AA.VV., Droit de l'informatique, cit., 1511 s.).

È, inoltre, superfluo ritornare sulla duttilità della formulazione a compasso allargato di cui all'art. 635 c.p. («chiunque disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili...»), che consente alla norma sul danneggiamento di operare – nel rispetto del divieto di applicazione analogica – in una vasta gamma di fattispecie, compreso il mero sconvolgimento della funzionalità della cosa (questa interpretazione è ribadita nella motivazione della sentenza in rassegna; sulle nozioni di deterioramento e inservibilità, cfr. MANTOVANI, Danneggiamento e deturpamento di cose altrui, voce del Digesto pen., Torino, 1989, III, 312 e ASSUMA, Danneggiamento, voce dell'Enciclopedia giuridica Treccani, Roma, 1988, X, 2, il quale chiarisce, a proposito dell'inservibilità, che «tale forma di danneggiamento [...] non modifica l'identità fisica o economica della cosa né la sottrae alla disponibilità dell'avente diritto, ma ne pregiudica l'utilizzabilità rispetto alla destinazione naturale»).

D'altronde, non si può non condividere quanto ribadito dalla Corte d'appello di Torino secondo la quale «la nozione di cosa nelle fattispecie dei reati contro il patrimonio [...] assai più elastica di una mera e stretta materialità [rectius: corporalità] (e basti pensare all'estensione verso le energie di cui all'art. 624, cpv., c.p.)». Inoltre, se è vero, come ritiene PICOTTI, op. ult. cit., 973, che il concetto di software è estraneo alla nozione di energia, non è altrettanto vero che quest'ultima sia estranea alle tracce magnetiche che lo rappresentano (secondo autorevole dottrina, è ritenuto configurabile

il danneggiamento di energie, ad es., tramite dispersione, così per l'energia elettrica: v., in questo senso, MANTOVANI, op. cit., 311).

Più problematici appaiono, almeno a prima vista, i profili legati alla sussistenza dell'elemento soggettivo del reato. Infatti, a chi, come chi scrive, rivendica la praticabilità dell'art. 635 c.p., si potrebbe obiettare che il dolo del sabotatore si rivolge al dato informatico e non alla traccia magnetica che ad esso corrisponde. Un problema analogo si pone per la riconducibilità del c.d. furto di tempo-macchina nell'alveo dell'art. 624, cpv., c.p. (furto di energie). Se anche non fosse possibile riprendere la logica di un'elegante tesi prospettata, per questa diversa fattispecie, a favore dell'applicazione della norma da ultimo menzionata (v. MANTOVANI, op. cit., 892 s.), il problema si risolverebbe, comunque, nella necessità di provare la consapevolezza, da parte dell'agente, di danneggiare il supporto oltre che il dato e non in un'esclusione a priori dell'integrazione dell'elemento soggettivo della condotta criminosa. Non sembra, peraltro, si tratti di una probatio diabolica; infatti, appare assai probabile che colui il quale sia capace di impartire all'elaboratore istruzioni distruttive di dati informatici possieda cognizioni informatiche abbastanza elevate e sia, perciò, perfettamente cosciente del fatto che questo tipo di condotta si risolve in un'alterazione del supporto su cui essi sono memorizzati.

In verità, quest'ultimo profilo è rimasto in ombra sia nella sentenza di primo grado che in quella d'appello su riportata. A ben guardare, ciò può essere dipeso dal fatto che il pretore torinese aveva individuato l'oggetto del reato non nel dato informatico (lato sensu inteso) in sé, né nel suo supporto materiale (che rimane riutilizzabile), ma nella funzionalità del «sistema informativo» costituito dal connubio inscindibile di software, basi di dati e hardware. Al di là della messa a fuoco dei profili soggettivi sopra evidenziati, questa nozione, coniata nella sentenza di primo grado, può forse sembrare impalpabile, e tuttavia risulta il frutto di un ragionamento (peraltro non compiutamente sviluppato) sostanzialmente esatto.

Occorre risalire a monte del problema e chiedersi quale sia il bene giuridicamente rilevante e meritevole di protezione (penalistica) di fronte ad aggressioni di questo tipo. A questo punto è necessario fare una distinzione di fondo tra programmi e basi di dati. Come accennato nelle sentenze dei giudici torinesi nelle fattispecie di sabotaggio di programmi, non è la lesione o distruzione di un'opera dell'ingegno – al di là del sostrato civilistico che una tale qualificazione del programma possa avere – a venire in evidenza, se non in casi limite (in astratto, non è mai configurabile un danneggiamento, in senso stretto, dell'idea; tuttavia, ad es. in campo artistico, quando vi è un'immedesimazione assoluta tra corpus mysticum e mechanicum, la lesione di quest'ultimo priva per sempre il fruitore dell'opera d'arte, compresa l'idea che essa esprimeva; un tale grado di immedesimazione non vale per altre opere dell'ingegno, ad es. per quelle di carattere letterario, cui si vuole sia assimilabile, ai nostri scopi, l'opera di natura scientifica come il programma per elaboratore).

Al contrario, è proprio la funzionalità del supporto-programma (che si traduce nella capacità del computer di svolgere date operazioni) il bene giuridicamente meritevole di tutela. Ciò è avvalorato dal fatto che, nella maggioranza dei casi, l'utente del software non entra nemmeno in contatto con (e quindi non viene in possesso del) la struttura logica del programma, mentre fruisce esclusivamente delle capacità operative che quest'ultimo dà al calcolatore. Per intenderci, se qualcuno mi danneggia la calcolatrice tascabile (mettiamo, avvicinandovi un grosso magnete), non mi lamenterò della lesione dell'idea custodita nella sua memoria, ma della sua diminuita funzionalità.

Per converso, nelle basi di dati l'oggetto della tutela è costituito dalla possibilità per il legittimo fruitore di accedere all'informazione ovvero di mantenere integra la sua «memoria artificiale». Posto che anche per tali informazioni non si può parlare di danneggiamento in senso stretto, la strada più agevole appare quella di una tutela del mezzo per accedervi ovvero dell'unità inscindibile

di supporto, software e dati stessi (non bisogna dimenticare che, nella fattispecie in esame, le banche di dati non erano state direttamente intaccate, ma lo sconvolgimento del programma atto a gestirle le aveva rese, in concreto, inaccessibili). La prospettiva di una tutela, per così dire indiretta, di questo tipo di informazione non deve punto meravigliare, anche perché, de lege ferenda, una norma penalistica che si dovesse incaricare di una copertura diretta del dato verrebbe a posarsi su fondamenta civilistiche men che solide (a questo proposito, interessanti spunti in margine alla tutela dell'informazione si rinvengono in ZENO ZENCOVICH, Cosa, voce del Digesto civ., Torino, 1989, IV, 453 s.).

Se si accetta una tale ricostituzione, non vi sono problemi di risarcibilità del danno derivanti dalla divaricazione in termini patrimoniali tra dati informatici e supporti che li contengono (all'operatività dell'art. 624 c.p. nel caso di furto di tempo macchina si oppongono attriti di questo genere; cfr., sul punto, MANTOVANI, op. cit., 893, il quale, peraltro, si appella, per superare queste difficoltà, ad un'interpretazione estensiva del nesso di causalità tra reato e danno civile risarcibile). Il danno, infatti, viene arrecato alla funzionalità dell'unicum costituito da supporto, software e dati. Inoltre, la modesta entità del danno patrimoniale sembra non costituire di per sé un motivo per escludere la sussistenza del reato di danneggiamento (v., in questo senso, Cass. 7 febbraio 1978, Vacchieri, Foro it., Rep. 1978, voce Danneggiamento, n. 4; 8 novembre 1982, Fornasiero, id., Rep. 1984, voce cit., n. 3).

L'ambito di questi rilievi è limitato ad una delle forme di sabotaggio del software (ben più ampio spazio richiede un'indagine su sabotaggi telematici virus et similia); sembra, comunque, che almeno essa rimanga nei confini del reato di danneggiamento.

ROBERTO CASO