

## RICERCHE

## ASSICURAZIONE E SOFTWARE

## SOMMARIO

1. Premessa. — 2. Tipologia ed analisi dei rischi informatici. — 3. L'affidabilità del *software* ed i rischi ad esso connessi. — 4. I tipi di copertura assicurativa per il *software* a disposizione dell'utente informatico. — 5. L'assicurazione e le *software houses*. — 6. Conclusione. L'assicurazione come strumento di tutela per l'utente.

## 1. PREMESSA

Anche se non si ritiene il linguaggio elettronico una sorta di « terza fase » nella storia della comunicazione parlata<sup>1</sup>, oggi giorno l'informazione è innegabilmente una forma di potere e di produzione. Il *computer* e la sua metodologia funzionale hanno facilitato l'evoluzione sociale da un'economia industriale, costituita da beni materiali, ad un'e-

conomica post-industriale, di servizi e informazione. Ci si aspetta, di conseguenza, che la legge intervenga nel settore, ridefinendo i rapporti fra gli individui e i gruppi, le relazioni tra enti, i diritti e i doveri di ognuno verso gli altri<sup>2</sup>.

Gli ordinamenti nei paesi a capitalismo maturo si sono mostrati più sensibili, in proporzione al grado di sviluppo raggiunto dall'informatica, verso una serie di problematiche che si riconnettono, in ultima analisi, alla disciplina e al controllo sociale dell'elaboratore elettronico. Ormai la discussione su questi temi è stata condotta con ampiezza tale da far accettare come luogo comune l'affermazione secondo cui l'informatica non è tecnica politicamente neutra, ma anzi è partecipe di una dinamica che conferisce maggiori poteri ai centri che del potere sono gli effettivi detentori (enti statali, grandi imprese)<sup>3</sup>. Tuttavia sarebbe oltremodo riduttivo identificare il diritto dell'informatica con la protezione della *privacy* o dei dati personali: esistono infatti anche ulteriori settori in cui informatica e diritto interagiscono, fra cui alcuni di carattere più specificamente civilistici<sup>4</sup>. Tra questi ultimi riveste particolare interesse l'aspetto relativo alle tecniche di gestione del rischio collegato all'utilizzazione di sistemi di elaborazione elettronica, sinora poco approfondita dalla dottrina.

È sin troppo ovvio sottolineare come gli elaboratori elettronici siano frequentemente usati per compiere operazioni di delicatezza tale che un'eventuale disfunzione può seriamente danneggiare, e talvolta annientare, l'utente sul piano commerciale<sup>5</sup>. Se, dunque, un sistema *edp* può costituire un punto nevralgico della gestione dei rischi che si incontra-

<sup>1</sup> Come, ad es., fa FROSINI, *Il diritto dell'informatica degli anni '80*, in *Riv. trim. dir. pubb.*, 1984, p. 390 ss.

<sup>2</sup> In questo senso, cfr. ALPA, *Il diritto dei computers*, in questa *Rivista*, 1985, p. 55 e SCOTT, *Computer Law*, New York-Chichester-Brisbane-Toronto-Singapore, 1985, par. 1.1.

<sup>3</sup> L'osservazione è di LINANT DE BELLEFONDS, *L'informatique et le droit*, Parigi, 1981, p. 52.

<sup>4</sup> Quali, ad esempio, quelli relativi alle tecniche di contrattazione e distribuzione del rischio nei c.d. « contratti informatici ». Su questo argomento, si veda a titolo indicativo G. ALPA (a cura di), *I contratti di utilizzazione del computer*, Milano, 1984, e in precedenza ALPA, *I contratti di utilizzazione dei computers*, in *Giur. it.*, 1983, IV, c. 42 ss.; nonché ROSSELLO, *I contratti dell'informatica*, in *Giur. it.*, 1984, IV, 145 ss.

<sup>5</sup> Caso paradigmatico, descritto anche in R.L. BERNACCHI, D.M. DAVIDSON and A.R. GROGAN, *Computer System Procurement*, 30 (1981) *Emory Law Journal*, p. 395 s., è *Triangle Underwriters, Inc. v. Honeywell, Inc.* La Triangle Underwriters, in affari ormai da più di quaranta anni, era una fiorente società che forniva un'ampia rete di servizi come agente generale per numerose compagnie di assicurazione. Contattata da rappresentanti della Honeywell, fu convinta a sostituire il proprio sistema IBM di elaborazione dati: ma il sistema Honeywell non funzionò mai perfettamente, né si riuscì a ripararlo. In capo ad un triennio, la Triangle Underwriters fu costretta a chiudere. Solo dieci anni dopo l'installazione del sistema *edp* difettoso la società riuscì ad ottenere un risarcimento, anche se molto limitato, attraverso un'azione intentata sul piano dei *torts* per *fraud*: ogni rimedio di tipo contrattuale era stato infatti bloccato dalle limitazioni imposte nelle clausole sottoscritte. Più in generale sul problema v. ROSSELLO, *La responsabilità da inadeguato funzionamento di programmi per elaboratori elettronici. Aspetti e problemi dell'esperienza nord-americana*, in *Riv. critica dir. priv.*, 1984, p. 123 ss.

no nell'esercizio di un'impresa, è essenziale per l'azienda valutarne l'affidabilità, sia come complesso, sia nelle sue singole componenti, allo scopo di ottenere una posizione il più possibile « sicura ». E tale « sicurezza » è raggiunta solo quando si sono approntati gli strumenti per evitare danni che impediscano la prosecuzione « normale » dell'attività, o per porre dei rimedi una volta che i danni stessi si siano ormai verificati. Ciò ha comportato lo studio e lo sviluppo di varie tecniche per affrontare e gestire le voci passive potenzialmente connesse con l'impiego dell'*electronic data processing*.

In primo luogo, la perdita va prevenuta, predisponendo idonee misure di sicurezza. Da questo punto di vista, nel settore informatico, l'utenza di un certo livello si mostra sensibile verso il problema della difesa (attiva e passiva) rispetto ai vari rischi ipotizzabili, anche grazie all'intensa attività di case costruttrici e ditte di consulenza.

In secondo luogo, e cioè nel caso in cui si interrompa comunque l'attività di elaborazione, vanno apprestate misure di emergenza, strutturate secondo un piano che consenta di continuare l'attività stessa o quantomeno di limitare le conseguenze di una sua interruzione<sup>6</sup>.

Infine, una copertura assicurativa può rappresentare un adeguato strumento di tutela rispetto ad un danno ormai avvenuto, e ciò non solo per l'utente, ma anche per il fornitore, tanto di *hardware* che di *software*. Con l'assicurazione, l'incidenza economica della perdita viene parzialmente trasferita su un'altra parte (la società assicuratrice), e l'assicurato ha la possibilità di tradurre in una cifra fissa (il premio) il valore economico del rischio che, se realizzato, potrebbe annientarlo economicamente.

Già una ventina d'anni fa il mercato assicurativo iniziò ad avvertire la necessità di coperture strutturate appositamente per il settore dell'informatica, forse anche in considerazione del fatto che le imprese d'assicurazione sono tra i maggiori utenti di sistemi *edp*<sup>7</sup>.

## 2. TIPOLOGIA ED ANALISI DEI RISCHI INFORMATICI

L'impiego dell'informatica talvolta può semplicemente ampliare, da un punto di vista quantitativo, la portata di un evento lesivo, ma, proprio per la varietà delle sue applicazioni, per la sua capillare diffusione, per la stretta dipendenza che si viene a costituire tra utenti ed elaborazione, può spesso contribuire alla creazione di rischi nuovi e di nuovi tipi di danno. In sé e per sé, la gravità del rischio connesso all'introduzione ed applicazione del *computer* in una qualsiasi attività non è un dato costante, ma una variabile determinata da una molteplicità di fattori (la struttura aziendale, l'impostazione conferita al centro di elaborazione, l'integrazione tra i vari rami produttivi, il tipo di impresa, e così via) che determinano a loro volta il livello di dipendenza dalle metodologie informative. Parallelamente, il concetto di « rischio informatico » non è suscettibile di definizione unitaria, né di una classificazione precisa entro i tradizionali rami assicurativi, in quanto può investire contemporaneamente più settori o esser-

<sup>6</sup> Sul punto, cfr. la relazione di FANTECHI, *Il piano di emergenza per l'edp* tenuta nel corso del convegno *Risk management e computer crimes* svoltosi a Carrara il 22-23 settembre 1983. Secondo l'autore, il piano di emergenza deve contenere l'attenta descrizione delle azioni da intraprendere, delle risorse da impiegare e delle procedure da applicare prima, durante e dopo il verificarsi di un evento « imprevisto » che interrompa la capacità elaborativa di una azienda. Gli elementi fondamentali del piano debbono in primo luogo determinare le esigenze da soddisfare e individuare le risorse più importanti, nonché pianificare le risorse critiche e definire le responsabilità gravanti sugli interessi. Da ultimo, va predisposta la documentazione scritta di tutte le procedure, documentazione che deve essere accessibile a tutti. Cfr. anche NORMAN, *Computer Insecurity*, Londra-New York, 1983, p. 326 ss.

<sup>7</sup> Le attività assicurative, per la prevalenza di lavoro amministrativo connesso alla gestione di innumerevoli contratti e pratiche per danni, nonché alle procedure contabili e fiscali da espletare, si prestano in misura considerevole all'automazione e all'informatizzazione: in effetti, le maggiori imprese assicuratrici dispongono di perfezionati centri di elaborazione dati e di complesse ed articolate reti periferiche. Questo dato di fatto fa sì che, in relazione alla gestione del rischio informatico, l'assicuratore si trovi in una situazione analoga a quella della sua cliente.

L'osservazione è tratta dalla relazione di COPPOLA DI CANZANO, sul tema *Esperienze internazionali in materia di rischi dell'informatica*, tenuta nel corso del terzo convegno *Industria e assicurazioni* dal titolo *Informatica e assicurazione*, svoltosi a Villa Manin di Passariano il 15 aprile 1983. Del dibattito è stata fornita una sintesi nell'articolo di BATTISTIG, *L'informatica e l'assicurazione*, in *Ass.*, 1983, p. 197 ss.

ne completamente estraneo, tanto da rendere necessario elaborare, *tout court*, nuove configurazioni. In ogni caso, all'interno della generica categoria identificata dalla espressione « rischio informatico » si possono operare alcune distinzioni fondamentali<sup>8</sup>.

La prima attiene alla *natura del rischio*. L'evento lesivo, infatti, può consistere in un danno (accidentale o meno e di carattere materiale) alla macchina o ai supporti di elaborazione, oppure può derivare dall'uso stesso dell'informatica, senza un sinistro in senso fisico al *computer* o ai programmi, come nel caso di errori o di uso fraudolento dell'elaboratore. Nel primo caso, il rischio viene qualificato come di natura *diretta*, nell'altro, si parla di rischi per perdita *indiretta*.

Un altro modello di analisi, più articolato, prende in considerazione i vari *tipi di copertura* assicurativa ipotizzabili. Entro tale schema viene in primo luogo in rilievo l'assicurazione dei danni a macchine e supporti di informazione: cioè la traduzione, nel settore informatico dei classici rischi *property*. Tale copertura può venire estesa anche ai danni, di tipo consequenziale, provocati dalla c.d. « interruzione di esercizio » coincidenti con le perdite economiche (lucro cessante) connesse al mancato uso dell'elaboratore<sup>9</sup>. Un diverso tipo di copertura, già noto nella prassi ma soggetto ad uno sviluppo continuo e peculiare, è connesso alla concreta possibilità di provocare danni a terzi (imprese, clienti

o dipendenti) che comportino una responsabilità civile dell'azienda utilizzatrice o produttrice del sistema *edp* o di parti di esso. Ma il settore più innovativo di tutela assicurativa è quello relativo ai c.d. rischi « infedeltà », vale a dire per uso fraudolento o criminoso del *computer*. Tale problematica assicurativa si riconnette a quella più generale del c.d. *computer crimes*<sup>10</sup>.

Riassumendo, quindi, si può dire che, dietro la generica espressione « rischio informatico », si distinguono per lo meno quattro distinte casistiche, a seconda che il rischio: *a*) sia legato alla macchina come bene economico; *b*) sia di tipo « indiretto », connesso alle conseguenze che l'interruzione dell'attività dell'elaboratore comporta a carico dell'utente; *c*) inerisca alle conseguenze di tutto ciò su altri soggetti, per cui si origina un problema di responsabilità civile per l'utente o per il fornitore; o infine *d*) derivi dall'uso illecito del *computer*.

Va precisato, inoltre, che ogni evento lesivo, qualunque sia l'area cui è astrattamente riconducibile, ha potenzialmente conseguenze molteplici (perdite finanziarie « secche », danni materiali, risarcimenti da corrispondere), spesso concomitanti e con incidenza differenziata. Comunque, le conseguenze più gravi di un guasto o dell'indisponibilità (qualunque ne sia la causa) di un sistema *edp* non sono quelle di tipo diretto, costituite dalla perdita (totale o parziale, definitiva o temporanea) di un valore patrimoniale e di un investimento dell'impresa. Se i componenti informatici rappresentano costi spesso ingenti nel bilancio di un'azienda, la loro effettiva incidenza economica risiede nel ruolo essenziale svolto nell'attività di gestione o di produzione, per cui un funzionamento insufficiente o inadeguato si traduce velocemente nell'insufficienza e nel peggioramento di quest'ultima. Le conseguenze più preoccupanti di una disfunzione del *computer* sono, certo proprio quelle di tipo « indiretto », essendo in questa dimensione che si valuta il livello reale e l'incidenza effettiva del rischio connesso con l'impiego dell'informatica. La valutazione di tale rischio appare estremamente difficoltosa nel campo considerato, sia perché è coinvolta una larga parte dell'attività aziendale, sia perché l'analisi deve essere inter-

<sup>8</sup> Cfr. le relazioni tenute al sopracitato convegno, nonché gli studi allegati al volume AA.VV., *Informatica e assicurazioni*, Trieste, 1983, che riproduce atti e contributi al convegno stesso, cui adde ora G.B. FORLINO, *Assicurazione e diritto informatico: i contratti assicurativi di base*, in G. ALPA-V. ZENO-ZENCOVICH (a cura di), *I contratti di informatica*, Milano, 1987, p. 361.

<sup>9</sup> Da un punto di vista teorico, tali perdite potrebbero però essere oggetto di un'assicurazione indipendente ed autonoma, e non essere soggette, come è invece nella prassi, ad una mera estensione di copertura.

<sup>10</sup> Il rischio « infedeltà » ha un connotato di estrema pericolosità per le banche e gli istituti finanziari in genere. Questi enti sono tra i primi (e maggiori) utilizzatori di *computers*, e perciò sono tra i più esposti ai c.d. reati elettronici. Tali problemi sono comunque suscettibili di estensione a tutte le organizzazioni che si servono del *computer* nella loro attività aziendale. Sul tema si è tenuto un convegno a Roma, il 30 aprile 1985, dal titolo *Computer crime: una concreta strategia di difesa*. Del convegno è data una sintesi in BICO, *Computer crime: un nuovo tipo di rischio*, in *Ass.*, 1985, p. 138 ss.

settoriale<sup>11</sup>. In generale, tale operazione consiste nel reperire strumenti o dati e nel disporne per decidere se investire o meno in contromisure<sup>12</sup> dal momento che il valore del rischio va sempre confrontato con il costo di eventuali rimedi. Data la loro novità, i rischi informatici non hanno però ancor supporti certi, di tipo statistico, utilizzabili a tale scopo<sup>13</sup>. A ciò va aggiunto che, mentre le cause produttive del danno possono essere enucleate con una certa facilità, le conseguenze sono più difficilmente prevedibili il che, come si vedrà, è sicuramente elemento condizionante quando si tratta di determinare la somma assicurata e premi assicurativi.

Va comunque sottolineata l'estrema importanza che lo studio e l'analisi del rischio informatico riveste nell'acquisizione di un sistema *edp*. Dal momento che un sistema di elaborazione dati rappresenta un investimento di notevole entità economica, le operazioni relative dovrebbero essere strutturate e studiate in modo da garantire all'utente la migliore utilizzazione possibile. È superfluo richiamare qui la crucialità della fase di negoziazione e delle trattative allo scopo di razionalizzare *ab origine* la distribuzione del rischio contrattuale relativo alla utilizzazione del computer<sup>14</sup>, ma è opportuno evidenziare il ruolo che in tale fase può giocare il *risk manager*. È stato suggerito<sup>15</sup> che nella fase preliminare alla stipulazione del contratto dovrebbero intervenire per lo meno cinque persone: un delegato alla direzione generale, in rappresentanza dell'impresa; il capocentro, che dovrà gestire il sistema informatico; un esperto di informatica esterno all'impresa, come consulente tecnico; un giurista per la consulenza legale; un rappresentante dei lavoratori direttamente coinvolti all'automazione. La loro partecipazione alla fase di preparazione del contratto ha il precipuo scopo di consentire non solo un'intesa preventiva sull'utilizzazione del computer in azienda, ma soprattutto (mediante la precisa individuazione della dimensione assunta dall'informatica nell'attività in questione) la migliore impostazione alla successiva negoziazione. Nelle trattative condotte successivamente il *risk manager* dovrebbe svolgere un ruolo fondamentale<sup>16</sup>. Le parti dovrebbero procedere all'individuazione dei ri-

schì: il *risk manager*, parallelamente, avrebbe il compito di indicare man mano i sistemi preventivi e, in genere, protettivi, precisandone il costo, nonché di fornire assistenza nella delimitazione e nell'imputazione delle responsabilità connesse. Operando in questo senso, il *risk manager* potrebbe non solo segnalare all'utente la copertura assicurativa più adatta per tutelarsi dalle conseguenze di un inadeguato funzionamento dell'elaboratore, ma esercitare pressione affinché analoga copertura sia imposta, con una previsione *ad hoc* nel testo del contratto, a carico del fornitore. In quest'ultimo caso, il costo della copertura finirà comunque per gravare sull'utente, sotto forma di maggiorazione del prezzo: ma l'utente ne avrà ugualmente vantaggio, in quanto il controvalore del rischio costituirà un dato certo, e le re-

<sup>11</sup> Cfr. la relazione di ASCHIERI, *La sicurezza dei dati* al già citato convegno *Risk management e computer crimes*. L'autore ha compiuto alcuni chiarimenti sul meccanismo di valutazione del rischio. In breve, si può dire che l'entità, cioè il valore del rischio, è dato nella sua forma elementare dal valore del bene in caso che questo venga perduto. Nel mondo aziendale, di solito tale valore è più complesso da calcolare: si devono infatti tenere presenti il valore/costo di ricostruzione del bene (e perciò anche le considerazioni finanziarie e di ammortamento), il valore/costo della penalizzazione prodotta dalla perdita, e, ancora, l'impossibilità di svolgere l'attività per un certo periodo o la perdita in immagine aziendale, e così via.

<sup>12</sup> L'osservazione è di NORMAN, *op. cit.*, p. 316.

<sup>13</sup> Cfr. NORMAN, *ibidem*.

<sup>14</sup> Cfr. su questo argomento v. le osservazioni di ROSSELLO, *I contratti dell'informatica. Spunti di riflessione di comparazione con l'esperienza statunitense e francese*, in ALPA (a cura di), *I contratti di utilizzazione del computer*, cit., p. 79 ss. (ma già in *Giur. it.*, cit., 145 ss.).

<sup>15</sup> LOSANO, *Corso di informatica giuridica*.

<sup>16</sup> È questo il suggerimento che si trova negli studi del convegno *Informatica e assicurazione*, cit., p. 197 ss., dove si precisa la funzione che tale esperto dovrebbe svolgere nella redazione del contratto *edp*. Infatti, anche se il buon contratto di informatica dovrebbe essere il più specifico possibile e delimitare con precisione le responsabilità a carico di utente e fornitore, non va sottovalutato il fatto che la forza contrattuale di quest'ultimo è preponderante, cosicché la maggior parte dei rischi è addossata alla controparte. Il *risk manager* è in grado, col suo apporto, di correggere tale tendenza, in quanto i rischi così individuati possono essere tradotti in un contratto dove gli interessi delle parti trovano un contemperamento più equo.

La figura del *risk manager* ha già conquistato in dottrina, soprattutto all'estero, un certo spazio. Cfr. a titolo indicativo NORMAN, *op. cit.*, p. 311 ss. Molteplici anche i riferimenti al ruolo del *risk manager* anche nel convegno *Risk management e computer crimes*, dove si sono svolte molte considerazioni, di carattere tecnico e pragmatico, sulla sua attività.

sponsabilità del fornitore non saranno limitate o escluse nelle clausole del contratto.

### 3. L'AFFIDABILITÀ DEL SOFTWARE ED I RISCHI AD ESSO CONNESSI

Il problema dell'affidabilità di un sistema *edp* nel suo complesso porta inevitabilmente a considerare in prima analisi l'affidabilità del *software*. Infatti, mentre l'*hardware* ha ormai raggiunto una sicurezza quasi completa, pare invece impossibile mettere a punto un programma senza errori. C'è chi parla di una proporzionalità tra il tempo di impiego del *software* e la quantità di errori scoperti<sup>17</sup>, ed è stato calcolato che circa il 40% delle installazioni fallisce per lo più in conseguenza di disfunzioni dei programmi applicativi<sup>18</sup>. Nella valutazione di tale dato, va anche considerato il ruolo fondamentale acquisito dal *software* nel patrimonio del sistema informativo<sup>19</sup>, che rende facilmente intuitibili le conseguenze di inadeguatezza o disfunzioni nel caso in cui l'errore concettuale inserito nel programma durante la sua progettazione ed attuazione venga scoperto quando il progetto è in fase avanzata, e sconta ormai ingenti costi di investimento. D'altro canto, non è molto agevole definire con esattezza che cosa si intenda per « correttezza » di un programma, in quanto non è affatto semplice separare l'elemento formale dall'inadeguatezza sostanziale.

<sup>17</sup> L'osservazione è di NORMAN, *op. cit.*, p. 11.

<sup>18</sup> Si veda la dichiarazione resa in questi termini dal perito del compratore nel caso *Chatlos System, Inc. v. National Cash Register Corp.*, 479 F. Supp., 738, 748 (DNJ 1979), aff'd, 635 F 2d 1081 (3d Cir. 1980).

<sup>19</sup> Il rapporto di costi tra *hardware* e *software* sta decrescendo nel tempo, con una progressiva erosione ad opera del mercato della piccola informatica nei confronti di quello di maggiori dimensioni. In effetti, la maggioranza dei programmi in uso presso i centri elettronici è di piccola mole: si è assistito, cioè, ad una progressiva decentralizzazione del ruolo svolto dalla funzione *edp*. Questa rilevazione è da mettere in relazione col fatto che la maggior parte dei problemi suscettibili di automazione non è di eccessiva complessità, e favorisce l'avvicinamento capillare alla utenza. In un sistema così strutturato, il *software* viene acquisendo una sempre maggiore rilevanza.

<sup>20</sup> Cfr. NORMAN, *op. cit.*, p. 292.

<sup>21</sup> Le osservazioni sono di NORMAN, *ibidem* (e p. 304), ma v. anche ROSSELLO, *I contratti nell'informatica*, cit., 152 ss.

In sintesi si può dire che un programma, per funzionare in modo soddisfacente, dovrebbe fare quello che il programmatore voleva facesse. Il programmatore, a sua volta, dovrebbe scrivere un programma in grado di assecondare perfettamente le richieste del committente. Sempre sul piano ideale, poi, il committente dovrebbe saper formulare una richiesta esattamente corrispondente a ciò di cui ha bisogno. In questo modo, qualora il *software* operasse in modo appropriato, il committente avrebbe quanto gli serviva, né più, né meno<sup>20</sup>. Anche se nell'esempio si è considerata la confezione di un *software* « su misura » per il cliente, le osservazioni valgono anche per una licenza d'uso. Il licenziatario dovrebbe ricevere il *package* più adatto alle esigenze da lui precisate in sede di trattative, e il concedente dovrebbe individuare quanto risponde alle richieste di controparte. In tal modo, ed in entrambi i casi, il programma sarebbe corretto ed adeguato.

Il primo elemento di divergenza da tale quadro ideale consiste nel fatto che, nonostante l'onnipresenza del *computer*, l'elaboratore è spesso acquistato senza avere conoscenza completa e idee precise su quanto effettivamente si possa pretendere dalla macchina e, soprattutto, dal programma. Si riprenda l'esempio della commissione *ad hoc* di un *software*. L'analista (o il programmatore, nel caso non raro, soprattutto nelle organizzazioni minori, che le due figure coincidano) deve elaborare un certo numero di « specifiche funzionali » per descrivere quanto il programma deve fare in ogni circostanza: ma può non avere inteso quello che l'utente voleva, o può aver redatto specifiche ineffettuabili per il lavoro da svolgere. In ogni caso, l'errore nella redazione passa al programma, a meno che non vi sia un intervento estraneo a scopo di verifica: e di rado l'utente è competente al controllo<sup>21</sup>. Talvolta, inoltre, possono verificarsi situazioni che *a priori* potevano essere definite come impossibili, rare, ovvie e perciò da trascurare od omettere, rispetto alle quali falliscono anche i *tests* più accurati. Dato, poi, che un qualsiasi programma commerciale di una certa entità contiene centinaia o migliaia di singole istruzioni, e dato che i programmatori ne scrivono correttamente in media da

una decina a un centinaio ogni giorno, un programma dimensionato nell'ordine delle mille enunciazioni richiede qualche mese per essere messo a punto<sup>22</sup>. In questo lasso di tempo, più persone possono avere lavorato sul *software*, e diventa problematico ricostruire dove, quando e come si è immesso l'errore nel programma, allo scopo di individuare una precisa responsabilità<sup>23</sup>. Vi sono, infine, ipotesi di cattivo funzionamento del programma non addebitabili alla sua intrinseca inesattezza: un programma può essere formalmente corretto, ma scritto in modo tale per cui è difficile correggere un comando impartito erroneamente<sup>24</sup>. In questi casi, l'inadeguatezza del programma è vista in prospettiva ancora più sfumata: e si comprende chiaramente come non basti la correttezza formale, cioè il fatto che funzioni senza produrre risultati inattesi, perché il *software* sia soddisfacente.

Questa serie già consistente di ipotesi non esaurisce però la tipologia dei rischi connessi all'impiego del *software*. Esiste, infatti, tutta una casistica corrispondente alle fasi di gestione delle informazioni (raccolta, codifica, immissione, elaborazione, trasmissione, conservazione, uscita). Ognuno di questi « anelli » nell'immaginaria catena che dai dati iniziali inseriti nel *computer* conduce sino all'*output* finale presenta livelli di rischio differenziati. Probabilmente, i punti più delicati sono costituiti dalla trasmissione, dove i numerosi passaggi di informazione tra strutture diverse, che necessitano di diverse misure di sicurezza, comportano la complessità e la molteplicità degli strumenti di protezione da mettere in opera, e dalla conservazione delle informazioni e dei programmi stessi, dove i rischi potenziali sono di varia natura. Ed in entrambi i casi di deve tener conto di un elemento molto importante: l'alta probabilità che intervenga una causa di disturbo esterna, data l'estrema vulnerabilità fisica dei supporti, e la relativa facilità di interruzioni o distorsioni nelle linee di trasmissione. Influenze esterne come radiazioni, cali di corrente elettrica, raggi cosmici possono alterare il messaggio o renderlo illeggibile durante il trasporto (anche la leggera curvatura di un disco può bastare a renderlo inservibile).

Nei confronti di queste possibili cause di malfunzionamento nel programma e nell'intero sistema elaborativo, l'utente è spesso privo di una tutela adeguata e dei mezzi per superare agevolmente il momento critico. Il rischio relativo finisce perciò col gravare a suo carico, mentre il fornitore può escludere o limitare la propria responsabilità, anche dal punto di vista aquilano, attraverso opportune previsioni contrattuali. Ed allora, uno strumento per gestire in modo adeguato tali rischi viene proprio dall'assicurazione.

#### 4. I TIPI DI COPERTURA ASSICURATIVA PER IL *SOFTWARE* A DISPOSIZIONE DELL'UTENTE INFORMATICO

Considerando la creazione e lo sviluppo delle polizze relative all'informatica in prospettiva diacronica, la prima espressione di sensibilità verso i problemi che l'introduzione del *computer* ha comportato nell'attività di impresa si è manifestata proprio in relazione alla esasperata delicatezza e complessità delle macchine, ed, in seguito, dei supporti di informazione. In effetti, si sarebbe potuto adattare la consueta polizza G.M. (Guasti Macchine) anche alle apparecchiature elettroniche, sia pure con opportune modificazioni. Invece, proprio in considerazione della particolarità del settore, si creò *ad hoc* la spe-

<sup>22</sup> Cfr. GEMIGNANI, *Product Liability and Software*, 9 (1981), *Rutgers Comp. & Techn. Law Journ.*, p. 185, il quale aggiunge come un *software* di complessità particolare impiega due o tre anni per essere sviluppato, e, nonostante l'ammontare degli sforzi e delle spese, può fallire egualmente, anche dopo verifiche estese.

<sup>23</sup> Secondo GEMIGNANI (*op. cit.*, p. 183 s.), le fasi in cui un errore può essere inserito nel programma sono quattro. La prima è la fase di elaborazione dell'algoritmo stesso; un'altra è quella in cui l'algoritmo viene tradotto in un linguaggio più elevato; la terza quando il programma sorgente è tradotto dal compilatore in linguaggio macchina; l'ultima fase, infine, è quella in cui il programma oggetto entra materialmente nella macchina; cfr. anche ROSSELLO, *La responsabilità da inadeguato funzionamento di programmi per elaboratori elettronici*, cit., p. 123 ss.

<sup>24</sup> L'esempio è in GEMIGNANI, *ibidem*, che fa riferimento anche al caso di un programma che manchi di controlli o della possibilità di duplicare operazioni critiche.

ciale polizza elettronica<sup>25</sup>, gettando così le basi per un nuovo ed autonomo ramo delle assicurazioni industriali.

Tale polizza, nata come « multirischi », e ora del tipo *all risks*<sup>26</sup>, copre tutti i danni diretti e materiali subiti da-

<sup>25</sup> Innanzitutto, la domanda di apparecchiature elettroniche è rappresentata da una categoria estremamente eterogenea, in cui si affiancano imprese commerciali, scuole, università, enti pubblici e così via, mentre di solito i potenziali richiedenti di una copertura G.M. non sono solo *managers* industriali. La situazione di mercato, strutturalmente atipica, ha perciò influito sull'atteggiamento dell'assicuratore, che ha dovuto trattare anche con persone non abituate a valutare l'opportunità di una garanzia assicurativa in tutti i suoi aspetti. In secondo luogo, le apparecchiature elettroniche in generale comportano una altissima concentrazione di valore in spazi ristretti, cosicché un eventuale guasto può compromettere l'intero impianto senza possibilità di intervento tempestivo.

Sul punto cfr. ROVELLA, *L'assicurazione delle apparecchiature elettroniche*, in *Dir. e pratica ass.*, 1976, pp. 638, 640 s.

<sup>26</sup> Il sistema risulta così più agevole per i clienti, in quanto la copertura « multirischi » abbisognava della accurata elencazione di tutte le possibili casistiche di rischio, e restavano perciò a carico dell'assicurato tutti gli errori e le omissioni nella determinazione dei limiti della copertura. Di fronte ad una nuova tecnologia non era affatto agevole identificare i rischi potenziali, con entità ed estensione non ancora precisata. Invece, con la polizza *all risks* spetta all'assicuratore fissare (anche se in via negativa e per esclusione) quando la copertura opera e quali rischi sono perciò ricompresi nella garanzia.

<sup>27</sup> Per una prima analisi delle diverse polizze predisposte dalle Compagnie italiane si v. la ricerca di F. STORACE, *La copertura assicurativa del rischio informatico*, in questa *Rivista*, 1986, 652. Nelle condizioni generali di assicurazione è di solito previsto l'obbligo, da parte dell'assicuratore, di riparare o sostituire il bene danneggiato con uno equivalente per prestazioni e valore di mercato. In genere, poi, il danno parziale viene risarcito a costi di fatturato di manodopera e pezzi di ricambio; la perdita totale, invece, secondo il valore corrente del bene danneggiato. L'estensione di garanzia consente il risarcimento a nuovo anche in caso di danno totale: è perciò molto ambita, anche se di solito viene concessa solo per apparecchiature non risalenti ad oltre tre anni prima o ancora in commercio o per cui, almeno, sono disponibili i pezzi di ricambio, dato l'alto rischio di obsolescenza dei *computers* e le frequenti variazioni di mercato. Queste osservazioni valgono, con le opportune modifiche, anche per il *software*.

Cfr. AA.VV., atti del convegno *Informatica e assicurazione*, p. 181 e s.

<sup>28</sup> Limitatamente però, alla parte colpita.

In base ai caratteri comuni, le esclusioni possono essere enunciate in cinque gruppi:

- 1) danni per dolo dell'assicurato, o per cui devono rispondere per legge o contratto i fornitori;
- 2) danni da usura, corrosione, etc., in quanto la indennizzabilità è limitata ai soli danni a carattere accidentale;
- 3) danni in occasione di eventi privi di interesse di copertura (guerra, tumulti, esplosioni nucleari, etc.);
- 4) danni per situazioni ambientali pericolose (erosioni, alluvioni, etc.);
- 5) danni per cui solo certi assicurati possono aver un qualche interesse (montaggio, smontaggio).

Cfr. AA.VV., *op. cit.*, p. 169 ss.

gli enti assicurati a seguito di un evento accidentale che non sia espressamente escluso dalla copertura.

In questo settore, la copertura per il *software* applicativo è configurata come un'estensione della garanzia principale, che riguarda invece l'*hardware* e il *software* operativo. Lo schema assicurativo va dalla perdita o dalla rottura del supporto in conseguenza di incendi, alluvioni, cortocircuiti, variazioni di corrente, scoppi, valanghe e così via, sino all'imperizia, negligenza ed errata manovra da parte dell'assicurato. Eventualmente, come nella polizza *hardware* corrispondente, la garanzia può essere ad eventi come sabotaggi, scioperi e terrorismo, o si può inserire la c.d. « garanzia valore a nuovo », molto richiesta<sup>27</sup>. Tra le molte esclusioni vanno poste in evidenza quelle relative ai danni dovuti al dolo dell'assicurato, al normale logoramento conseguente all'impiego prolungato, alle disfunzioni prodotte da difetti dei materiali utilizzati e da vizi di costruzione<sup>28</sup>, o dei quali l'assicurato era già a conoscenza al momento della stipula della polizza.

Con questa copertura viene risarcita la perdita del supporto e la spesa per la ricostruzione di dati ed informazioni. Non vengono invece in genere risarciti né la perdita del programma né il valore intrinseco delle informazioni, e cioè in definitiva, gli elementi che racchiudono in sé l'investimento economico più consistente a carico dell'utente.

Questa situazione è resa ancora più complessa se si osserva che la perdita di dati e programmi comporta sempre un certo numero di spese apportate proprio al fine di porre rimedio all'interruzione, anche se solo temporanea, nell'attività elaborativa.

Tenendo conto di tali elementi, la copertura assicurativa per danni diretti al *software* dovrebbe essere strutturata secondo quattro livelli. Si dovrebbero, cioè, prendere in considerazione sia il caso di perdita del supporto e di conseguente perdita delle informazioni (magari accompagnata dalla perdita dei programmi), sia il caso di distruzione di informazioni e programma anche senza perdita del supporto; in ultimo, andrebbero valutate anche le maggiori spese sostenute per ovviare, in questi frangenti, alla connessa paralisi dell'elaborazio-

ne<sup>29</sup>. Attualmente invece sono escluse dalla garanzia la perdita del *software* senza un danno materiale, la perdita dei programmi, e spesso anche le maggiori spese sostenute per proseguire l'attività, che vengono così annoverate come accessorio della copertura danni *hardware*.

Per quanto attiene alla perdita di un *software* senza un indizio palese, esso è un fenomeno certamente non raro, ma privo di possibilità di verifica sul piano fisico<sup>30</sup>. In effetti, l'esistenza di un « danno » materiale al supporto dà comunque modo di controllare l'effettività della lesione; mentre in caso contrario manca l'appiglio per valutare e quantificare il danno<sup>31</sup>. La perdita dei programmi poi, non è di solito risarcita sia per considerazioni pratiche, come nel caso precedente, sia per obiettive difficoltà di valutazione<sup>32</sup>. Il costo di ricostruzione delle informazioni è un elemento quantificabile e controllabile, dal momento che un assicuratore, valendosi di statistiche, può fissare il livello medio di costi che un centro per la ricerca di informazioni sostiene per la loro codifica ed immissione: non è però possibile fare altrettanto con un programma, di cui sarebbe necessario allo scopo conoscere il livello di aggiornamento e di manutenzione, l'utilità, le eventuali disfunzioni.

Tali costi possono essere conosciuti solo dall'assicurato, e non sono certo valutabili da un perito, per cui, dato che l'assicuratore avrebbe come sola indicazione la stima fatta prima del rischio dal cliente, la perdita del programma potrebbe offrire spunto a speculazioni illecite da parte degli utenti<sup>33</sup>.

Inoltre, i programmi sono di solito duplicati e conservati in zone di sicurezza, proprio come misura preventiva essenziale: ed allora un utente dovrebbe sempre poter disporre in qualsiasi momento di copie di riserva (*back up*) tenute « al sicuro » appunto in vista di simili evenienze. Nel caso, invece, di programmi non duplicati, e cioè acquisiti in base a licenza d'uso, dove clausole specifiche spesso vietano o limitano il numero di copie effettuabili del *software*, conservare tali copie è norma di diligenza per la stessa *software house* cedente. Ciò avviene anche in caso di sviluppo *software*, e non solo per sicurezza, ma anche per il valore di investimento di

energie intellettuali racchiuso nel programma.

In base a tali considerazioni, quindi, la somma assicurata è determinata dalla stima delle spese che il centro dovrà compiere per ricostituire le informazioni immagazzinate quale considerata prima del prodursi del rischio stesso, risultando pressoché impossibile procedere ad una verifica *a posteriori*<sup>34</sup>.

<sup>29</sup> Cfr. gli studi del convegno *Informatica e assicurazione*, cit., p. 238.

<sup>30</sup> *Op. ult. cit.*, p. 183.

<sup>31</sup> In Germania ed in Francia esistono però coperture in cui è previsto un caso di danno al *software* senza lesione al supporto: è la ipotesi del fulmine, che provoca campi elettromagnetici in grado di smagnetizzare il dischetto. Si tratta comunque di un fenomeno che in qualche modo può essere constatato. In Gran Bretagna alcune compagnie prevedono la copertura del costo di ricostituzione anche in caso di cancellazione accidentale. Tale garanzia è però concessa assai di rado, solo a clienti selezionati e con certi limiti di indennizzo. Tra l'altro, vanno adottate determinate misure di sicurezza nel ricovero di dati e copie, ed è anche prevista una franchigia, pari a circa quattro ore di lavoro del *computer*.

<sup>32</sup> Una delle poche polizze in cui non si differenzia il contenuto dal supporto, e perciò viene risarcita anche la perdita del programma, è quella giapponese. In Gran Bretagna sono stati compiuti studi in tal senso, anche se si sono presi in considerazione solo i programmi standard, tra l'altro con un risarcimento limitato al costo della registrazione di una copia di riserva. Il contratto, inoltre, andrebbe subordinato all'accertamento dell'affidabilità del cliente, a verifiche continue ed alla operatività di un contratto di manutenzione.

<sup>33</sup> Cfr. AA.VV., *Informatica e assicurazioni*, cit., p. 182 e s.

<sup>34</sup> Esistono vari sistemi per determinare tali costi. Una esauriente trattazione e il confronto tra le metodologie adottate nei diversi paesi europei è contenuta negli studi del sopra indicato convegno, di cui questa sintesi è largamente debitrice.

Un primo metodo è assai analitico. Il patrimonio informatico viene diviso in classi, a seconda del supporto e del tipo d'informazioni contenute (di base, variabili di passaggio, di parcheggio), e a ciascuna di esse viene attribuita una somma di riferimento, in cui viene inglobato anche il costo di acquisto del solo supporto.

Un altro sistema parte dall'analisi dei dati duplicati e dall'ubicazione delle copie. I costi in questi casi possono essere ridotti a quelli del supporto e a quelli di registrazione dei duplicati: grava così sull'assicurato il rischio di perdita sia della copia, sia dell'originale.

Un altro metodo prende in considerazione l'intero patrimonio informatico dell'azienda, ma all'assicuratore spetta fissare un limite al risarcimento, e ridurre di conseguenza il premio.

In tal modo, l'analiticità del primo metodo si accompagna alla minore dispendiosità del secondo, ma c'è il pregio di una valutazione globale del rischio.

Si può anche pervenire ad una stima in via statistica, grazie al costo medio di elaborazione di un *byte* (unità di misura dell'informazione digitale) moltiplicando per i *bytes* elaborati dal centro.

In ogni caso, vanno applicati alcuni correttivi per tener conto del sistema di archiviazione, della sicurezza e del deposito dei dati.



Inoltre, a sua volta determinata la somma assicurata, si devono valutare anche i connotati del rischio nella loro dimensione oggettiva, alla luce delle misure preventive messe in atto, dei sistemi di soccorso predisposti, dei

<sup>35</sup> Di solito vengono concessi sconti, anche di una certa entità, quando è prevista la conservazione dei duplicati in armadi resistenti al fuoco: in tal caso va controllato non solo dove sono collocati i supporti, ma anche la regolarità del posizionamento e le caratteristiche tecniche dei mezzi di allocazione.

<sup>36</sup> La necessità di servizi paralleli all'acquisizione di *software* non si apprezza solo in prospettiva assicurativa. Anzi, tali servizi (*software support, maintenance and training*) non sono semplicemente tra i maggiori benefici che si possono ottenere dal fornitore: sono, secondo l'espressione di DILLOWAY (*Purchasing Computer Software Products*, Cambridge, 1985, p. 13), quello che l'utente effettivamente acquista. Ora, da questo punto di vista, la manutenzione offerta per i programmi standard è capillare e diffusa, ed è apprestata dalla *software house* stessa. Invece, per i programmi confezionati *ad hoc* la *software house* di solito non assume alcun impegno esplicito di buona riuscita, ma si obbliga a prestare assistenza proprio come mezzo di correzione continua del programma. In questo contesto, diventa molto più delicato tenere distinto — come invece è necessario ai fini della copertura — il prodotto *software*, come bene di per sé finito, e i servizi connessi. Sulla manutenzione del *software* cfr. adesso ROSSELLO, *I contratti di manutenzione del software*, in G. ALPA-V. ZENO-ZENCOVICH (a cura di), *I contratti di informatica*, cit., p. 203.

<sup>37</sup> Ecco indicate alcune tra le voci più comunemente risarcite nei formulari:

- i costi per lavoro straordinario, festivo, etc. per il personale;
- costi per l'assunzione temporanea di personale straordinario o per consulenza;
- costi per noleggio di calcolatore sussidiario;
- costi di compatibilizzazione e avviamento del calcolatore sussidiario e adattamento dei programmi (recentemente introdotta anche in Italia);
- costi di trasporto di archivi, dati e programmi sul nuovo calcolatore sussidiario;
- costi per affitto di locali per le nuove macchine;
- costi di memorizzazione successiva di tutte le operazioni effettuate manualmente; e così via.

Tali costi sono di solito riferiti su base annua, e sono indicati dall'assicurato.

Le esclusioni generalmente attengono alle spese per modifiche, revisioni e migliorie eseguiti in occasione della riparazione o adattamento delle cose assicurate, al deterioramento e alla distruzione di materie prime, ai danni causati da limitazione dell'attività aziendale o da indisponibilità di mezzi finanziari. I costi dipendono dalle strategie prescelte per la prosecuzione dell'attività che possono andare dalla manualizzazione delle procedure, alla ricerca di un altro macchinario, agli accordi tra più aziende (c.d. *back-up contract*), al raddoppio del centro, o all'abbonamento ad un centro di continuità o di servizio (esperienza rivelatasi molto proficua negli USA). L'assicurato può richiedere limiti di risarcimento temporale per sinistro, con correlativa riduzione del premio da corrispondere; possono essere previste, inoltre, franchigie temporali o scoperti in percentuale del danno con un minimo in valore assoluto.

Cfr. AA.VV., *op. cit.*, p. 188 ss.; p. 239 ss.

metodi di controllo e, soprattutto, della conservazione dei supporti<sup>35</sup>. Nel caso (non frequente) in cui venga risarcita anche la perdita del programma, si deve tener conto della sua manutenzione. Di conseguenza, vengono esclusi dall'ambito assicurativo i danni di cui deve rispondere tale contratto o che, comunque, derivino dall'assistenza<sup>36</sup>.

Qualora si verifichi un evento riconducibile nell'ambito della copertura « danni diretti al *software* », l'aspetto sicuramente più problematico per l'utente è costituito dalle spese che bisogna effettuare per proseguire l'attività. Il mercato assicurativo europeo offre per questa ipotesi solo la garanzia « maggiori costi per la prosecuzione d'esercizio », per la cui validità è necessario che sussista sia la polizza « base » per la macchina, sia l'estensione di questa al *software*. La copertura, dunque, opera unicamente in riferimento ai danni risarcibili ai sensi della polizza elettronica: ed inoltre non viene concessa, in relazione ai possibili danni al *software*, da molte compagnie assicurative. Dal punto di vista dell'utenza, una simile limitazione alla possibilità di tutelarsi mediante assicurazione dalle gravose conseguenze di una lesione al programma appare per lo meno inopportuna, ma è, d'altro canto, conseguenza diretta dei problemi presentati dai meccanismi, e dalle circostanze, di risarcibilità del *software*.

In effetti l'assicuratore può intervenire, per quanto attiene alle misure da adottare per proseguire l'esercizio dell'impresa, solo sull'aspetto finanziario, e cioè sui costi da sostenere. In simili frangenti, le spese straordinarie sopportate devono essere documentate ed effettivamente essenziali per la sopravvivenza commerciale. Appare perciò comprensibile che, per talune compagnie d'assicurazione, non siano tali, ad esempio, le spese per la messa in opera di quelle copie che le norme di diligenza vuole apprestate e ben conservate da parte dell'utente<sup>37</sup>.

Sempre in considerazione della complessità e della delicatezza delle questioni relative alla risarcibilità del *software*, il mercato non offre per il programma l'equivalente di quella copertura per « danni da interruzione d'esercizio » che invece esiste con riferimento all'*hardware*. In effetti, una simile coper-

tura esige un certo grado di verificabilità e determinabilità *ex ante* del tipo di lesioni cui agganciare la risarcibilità del danno sofferto, e non può essere ancorata ad un numero impreciso di circostanze altrettanto imprecisabili, col pericolo per l'assicuratore di vedere confusa la demarcazione (che invece va tenuta ben distinta) tra rischi puri e rischi imprenditoriali<sup>38</sup>, e di dovere risarcire perdite che derivano da una gestione malaccorta o da particolari congiunture di mercato.

In questo contesto, è evidente che l'interruzione o la riduzione della produzione sono assicurabili solo quando la causa attenga alla sfera dell'accidentalità o, al più, sia annoverabile tra gli eventi naturali<sup>39</sup>. Perciò, se da un lato una garanzia estesa in questo senso appare molto appetibile nel settore informatico, dove proprio sul piano delle conseguenze si apprezza l'entità delle perdite connesse ad una disfunzione del sistema *edp*, dall'altro il mercato assicurativo europeo ha concordemente deciso che tale copertura sia agganciata alla sola polizza *hardware* di base. Di conseguenza, il danno che « interrompe » o « riduce » il valore dell'attività produttiva dev'essere risarcibile ai sensi della polizza relativa ai « danni diretti » alla macchina.

Va poi precisato che la copertura è stata strutturata secondo un sistema di indennizzo poco duttile ed elastico, soprattutto se riferito alla natura ed agli impieghi del *software*<sup>40</sup>, e non se ne prevede, almeno per ora, l'estensione al di fuori della polizza *hardware*. Inoltre, non risulta che essa conosca in Italia una rilevante diffusione. Il che dipende probabilmente non solo dalla struttura della polizza (che la rende idonea principalmente per utenti in grado di servirsi dell'opera di esperti nel definire i termini contrattuali e gestire il rapporto che ne deriva), ma anche da un limitato interesse della clientela. D'altro canto, va sempre rammentato che l'utente subisce le perdite più ingenti, qualora il sistema elaborativo funzioni in modo inadeguato, proprio su un piano indiretto ed in via consequenziale, a causa della riduzione o dell'arresto dell'attività imprenditoriale o a causa della responsabilità civile che da tale inadeguatezza può derivare a suo carico.

In quest'ultimo caso, si ritiene comunemente che l'impiego di mezzi tecnologici non muti i connotati, i parametri e i criteri di imputazione di tale responsabilità, ma aumenti solo il c.d. livello di esposizione al rischio, sicché basta semplicemente elevare i massimali di copertura, in modo da far fronte al maggior rischio di pregiudizio patrimoniale. Se invece il rendimento insufficiente del sistema dipende da un vizio intrinseco, se, cioè, la macchina è difettosa o il programma non è « corretto », esiste la possibilità di stipulare un'assicurazione: ma non da parte dell'utente, bensì del fornitore, di *hardware*, di *software* o di entrambi.

È bene, infine, ricordare che qualora il funzionamento carente dipenda dall'imcompetenza di chi è preposto a tale compito, non può esserci nessuna copertura assicurativa: si è, infatti, nell'ambito del rischio imprenditoriale e delle scelte che attengono alla gestione dell'impresa.

## 5. L'ASSICURAZIONE E LE SOFTWARE HOUSES

Si è ormai generalizzata la pratica che impone al licenziatario, in caso di locazione di impianto *edp*, di stipulare un'assicurazione per i danni eventualmente provocati al sistema oggetto della negoziazione. Lo stesso avviene nelle licenze d'uso di *software*, dove il cedente ha la esenzia primaria di circondare d'ogni possibile tutela il programma, in mancanza di quella sicura protezione

<sup>38</sup> Per l'applicazione al settore informatico della distinzione tra rischi puri, che producono solo perdite, ed imprenditoriali o speculativi, che possono dar luogo a perdite o guadagni, cfr. NORMAN, *op. cit.*, p. 311 ss. Si veda anche la relazione di MONALDO al convegno *Risk management e computer crimes*, dove, tra l'altro, si osserva come l'incidenza di un errore — di valutazione, progettazione od esecuzione — tenda ad aumentare il (solo) rischio imprenditoriale.

<sup>39</sup> È significativo, a questo fine, ricordare che il primo esempio di tale copertura si è avuto nell'ambito delle polizze contro i danni da incendio.

<sup>40</sup> Cfr. AA.VV., *op. cit.*, p. 192 ss., dove si trova un esame assai analitico della copertura, delle sue varianti e dei metodi di indennizzo.

giuridica che sarebbe invece necessario<sup>41</sup>.

Pare perciò molto opportuno che anche il fornitore si premunisca con una parallela assicurazione, soprattutto nel mercato del *software*. La grande espansione del settore ha fatto sì che gli opera-

tori siano in numero elevato ma variabile, spesso con breve durata commerciale e dimensioni economiche relativamente limitate<sup>42</sup>. Tutto ciò fa supporre (ed anzi temere) che nel momento in cui una di queste *software houses* fosse ritenuta responsabile di un qualche danno, e perciò dovesse corrispondere un risarcimento, essa potrebbe mancare delle disponibilità finanziarie necessarie, con la conseguenza di lasciare il danneggiato insoddisfatto<sup>43</sup>.

Una clausola appositamente inserita nel contratto, che imponga o attesti l'esistenza della copertura assicurativa da parte della *software house*, potrebbe rappresentare un utile mezzo di tutela per gli utenti *edp* (soprattutto se piccoli o medi) e un elemento di preferenza nella selezione di mercato.

Delle molteplici attività che possono essere svolte da una *software house*<sup>44</sup> interessa in questa sede il ruolo di fornitore di *software*. Tale attività, che si concreta dal punto di vista giuridico nella stipulazione di contratti di licenza d'uso o di sviluppo *software*<sup>45</sup>, viene ritenuta una prestazione di servizi. Infatti, benché talvolta il programma venga commercializzato come un prodotto, non è considerato tale dal mercato assicurativo<sup>46</sup>; e perciò non si ritiene utilizzabile da parte delle *software houses* quella assicurazione per responsabilità civile prodotti che invece è disponibile per i fornitori di *hardware*<sup>47</sup>.

I danni che una *software house* può provocare nella propria attività sono di varia natura, e di entità potenzialmente elevata. Di solito, comunque, nella pur vasta tipologia, tali « lesioni » non riguardano cose o persone, ma si traducono piuttosto in perdite puramente finanziarie<sup>48</sup>, originate da cause quali errori nella concezione dei programmi, errori materiali nell'immissione dei dati o, più genericamente, negligenza od imperizia.

Non tutti i rischi sono, ovviamente, assicurabili. Alcuni lo sono solo osservando certe condizioni<sup>49</sup>. Non possono essere assicurati, ad esempio, i danni causati agli elaboratori ed ai supporti materiali delle informazioni, che vanno coperti con la polizza elettronica; le conseguenze di impegni particolari eccedenti le obbligazioni di legge, come penali contrattuali; le pure garanzie

<sup>41</sup> Sulla licenza d'uso e la clausola *Indemnity and Insurance*, cfr. l'analisi di DILLOWAY, *op. cit.*, p. 74 ss. Sulla tutela giuridica del *software*, si veda per un'impostazione generale ALPA (a cura di), *La tutela giuridica del software*, Milano, 1985, con numerosi contributi di autorevole dottrina. Cfr. anche ROSSELLO, *La tutela giuridica del software nei primi orientamenti giurisprudenziali*, in questa *Rivista*, 1985, p. 103 ss., ove un'efficace sintesi dei vari problemi.

<sup>42</sup> Dal momento che la domanda supera di gran lunga l'offerta, ed il capitale necessario non è di elevata entità, il mercato del *software* appare piuttosto aperto. Cfr. HANSEN, *Software Distribution, Remarketing and Publishing Agreements*, 4 (1984) *Computer Law Journ.*, p. 630 ss.; LEGGIO, *Struttura della domanda e offerta edp e i suoi effetti nel rapporto contrattuale*, in *Riv. inf.*, 1985, p. 335 ss.

<sup>43</sup> L'osservazione è di DILLOWAY, *op. cit.*, p. 76.

<sup>44</sup> Ad esempio, consulenza, *audit*, formazione personale, assistenza tecnica, manutenzione.

<sup>45</sup> Sulle caratteristiche di tali contratti, la bibliografia appare ormai consistente. Si consenta di rinviare per un primo approccio ad ALPA, *I contratti di utilizzazione dei computers*, cit., c. 45 ss.; ALPA (a cura di), *I contratti di utilizzazione del computer*, cit., in cui si segnala sempre, ROSSELLO, *I contratti dell'informatica*, p. 79 ss.; e, per gli ordinamenti anglosassoni, MORGAN, *Computer Contracts*, Londra, 1979; DILLOWAY, *Purchasing Computer Software Contracts*, cit. (per le sole licenze d'uso).

<sup>46</sup> L'osservazione è di DILLOWAY, *op. cit.*, p. 75.

<sup>47</sup> Con tale polizza si coprono i danni provocati dall'*hardware* a consumatori ed utenti in genere, purché tali danni, rivolti a beni o consistenti in lesioni personali, trovino la loro causa in un difetto imputabile alla macchina. I difetti possono derivare sia da un'errata concezione o progettazione della macchina, sia da materiali inadatti utilizzati per la realizzazione concreta, da disfunzioni nella produzione, da un imballaggio non appropriato o da istruzioni sbagliate. L'assicuratore s'impegna a difendere il fornitore in sede penale e civile anche da richieste infondate: ma non sono coperte le conseguenze dannose di contenuto esclusivamente economico.

<sup>48</sup> DILLOWAY (*op. cit.*, p. 75) osserva che un esempio di lesioni a beni o persone cagionate da un programma può essere il crollo di un ponte, il cui progetto sia stato elaborato grazie ad un *computer*: ma, in tal caso, si potrebbe obiettare che il danno non è attribuibile al *software*, bensì al modo in cui esso è stato utilizzato. Probabilmente, sono ipotesi al riparo da critiche quelle citate in S. NY-CUM, *Liability for Malfunction of a Computer Program*, 7 (1979) *Rutgers Comp. & Techn. Law Journ.*, p. 1 ss., che comprendono tra l'altro uno scontro aereo causato dalla disfunzione del programma che controlla il radar e un disastro ferroviario provocato da analoghi motivi.

Per una impostazione generale sui problemi di responsabilità civile connessa all'uso dell'informatica, cfr. ALPA, *Responsabilità extracontrattuale ed elaboratore elettronico*, in questa *Rivista*, 1986, 387.

<sup>49</sup> Così AA.VV., *op. cit.*, p. 203 ss., da cui sono tratte le osservazioni che seguono.

di risultato, cui l'assicurato s'è impegnato<sup>50</sup>. Ancora, possono essere assicurati solo con versamento di un sovrappremio le conseguenze dannose connesse a ritardo o mancata esecuzione di un'obbligazione di cui è fatto carico all'assicurato<sup>51</sup> o le eventuali spese supplementari necessarie per rispettare tempi e termini della prestazione<sup>52</sup>. Si deve ancora osservare che l'individuazione dei rischi assicurabili non può essere compiuta conservando la nozione di « fatto accidentale » accreditata nelle tradizionali polizze r.c. Se il fatto accidentale è condizione per l'operatività della garanzia assicurativa, esso va ridefinito nel campo dell'informatica, dove esistono aspetti peculiari da tenere costantemente presenti. Connessa a tale problema è anche l'individuazione del periodo di garanzia, che si può astrattamente compiere con riguardo a tre momenti: il fatto generatore, il verificarsi del danno, la richiesta di risarcimento formulata nei confronti dell'assicurato. Siccome è possibile che intercorra un periodo di tempo apprezzabile tra « creazione » del danno e suo manifestarsi, non pare azzardato suggerire che, sia per fissare i limiti temporali della garanzia, sia per circoscrivere l'impegno finanziario dell'assicuratore, la migliore scelta consista nell'optare per il momento della richiesta di risarcimento<sup>53</sup>. Si potrebbero anche concedere estensioni temporali all'operatività della garanzia da parte dell'assicuratore, ad esempio in caso di cessazione d'attività dell'assicurato (il che comporta, com'è noto, il termine del contratto)<sup>54</sup>.

Una delle rare polizze specificamente studiate per l'informatica in questo campo esiste in Francia, dove gli assicurati sono all'avanguardia nello studio di questi problemi. Si tratta di una copertura concepita per le società aderenti al *Syntec* (« Camera sindacale delle società di servizi e consulenza informatica »), anche se la stipulazione del contratto è del tutto facoltativa. La copertura offre una garanzia strutturata in modo duplice per l'utente, in quanto copre non solo ogni rischio di responsabilità civile, qualunque sia la natura delle prestazioni fornite dalla *software house*, ma anche tutti i danni, sia patrimoniali, sia a persone o cose, persino in caso di responsabilità del centro per fatto dei sub-appaltatori, o nell'ipotesi di danni da mancato o ritardato adem-

pimento di obbligazioni conseguenti a morte o inabilità al lavoro del responsabile del prodotto.

Anche sul mercato inglese è presente una polizza particolare, detta « *Computer insurance policy* », composta da tre sezioni dedicate rispettivamente ai danni alle cose, all'interruzione di esercizio e alla responsabilità civile. In quest'ultima parte viene concessa copertura per i danni economici, subiti dall'assicurato o rivendicati da terzi, per qualsiasi atto di negligenza, errore, od omissione commessi dall'assicurato stesso o dai suoi dipendenti, con esclusione dei sinistri dovuti a frode o dolo, addebitati a società controllate dall'assicurato, causati da guasti meccanici ed elettrici, dovuti a diffusione di segretiazionali o brevetti.

Il mercato scandinavo presenta una polizza tra le più complete ed originali, con un livello qualitativo eccezionalmente elevato ed una struttura molto moderna. La polizza è articolata su sei sezioni, e cioè: danni a cose, interruzione di servizio, responsabilità, errori ed omissioni, infedeltà, uso fraudolento del *computer*. La terza sezione è a sua volta divisa in due gruppi di ipotesi: uno attiene alla r.c. terzi per danni fisici o malattie provocati a qualunque persona, nonché a distruzione o danneggiamento di proprietà di terzi; l'altro alla responsabilità civile verso i dipendenti durante il periodo di lavoro, comprese le eventuali spese legali che l'assicurato dovesse sostenere in relazione a questi eventi. La quarta sezione garantisce le perdite economiche in relazione a negligenza, errori ed omissioni, di cui l'assicurato si renda responsabile: non devono però essersi prodotte lesioni

<sup>50</sup> Il fornitore, come dimostrano le espressioni contenute nei formulari comunemente utilizzati nella prassi, tende a configurare gli impegni assunti come obbligazioni « di mezzi » e non « di risultato » (sul punto, cfr. ROSSELLO, *op. ult. cit.*, p. 98): cosicché la confezione e la locazione di programmi appaiono attività « assicurabili ».

<sup>51</sup> In tal caso, la garanzia può venire estesa a detti inadempimenti qualora essi non siano dovuti ad eventi riconducibili alla volontà dell'assicurato, ma siano derivati da fattori aleatori e fortuiti indicati espressamente in contratto.

<sup>52</sup> La prestazione di tale garanzia è subordinata al verificarsi di un evento, individuato, aleatorio e fortuito, cui siano ricollegabili le maggiori spese sostenute: altrimenti si invade l'area del rischio imprenditoriale.

<sup>53</sup> La *software house* è perciò coperta per tutte le richieste di risarcimento pervenute nel periodo di validità della polizza, il che è un indubbio vantaggio per l'utente.

<sup>54</sup> I dati che seguono sono tratti da AA. VV., *op. cit.*, p. 207 ss., nel capitolo dedicato alle « Analisi di mercato ».

corporali o danni alle cose, e sono del pari escluse anche le conseguenze di impegni assunti che non siano stati osservati per ragioni di affidabilità del sistema o dei programmi. La quinta e la sesta sezione riguardano rispettivamente i danni subiti a seguito di reati come appropriazione indebita, abuso di fiducia, frode o furto commessi da un dipendente anche contro un cliente (sempre, però, che l'assicurato debba risponderne), nonché i danni cagionati dall'uso del calcolatore da parte di terzi per scopi criminosi.

In Giappone vi sono due modelli assicurativi di responsabilità civile predisposti per le *software houses*. La polizza « *Data processor* » copre le perdite finanziarie causate ai clienti per mancanza di diligenza nell'adempimento delle prestazioni assunte, escludendo però ogni responsabilità derivante da errori od omissioni in fase di analisi, sviluppo o pianificazione d'un sistema o nella programmazione. A tale previsione si può derogare con un'apposita appendice alla polizza, anche se comunque sono poste notevoli limitazioni in termini di franchigia e di massimali di risarcimento. La polizza « *Data Processor Premises* » copre invece la responsabilità civile per lesioni fisiche o danni materiali a terzi dovuti a difetti strutturali o ad insufficiente manutenzione dei locali di proprietà dell'assicurato.

In Italia è disponibile un contratto tipo che copre la responsabilità civile dell'assicurato per danni patrimoniali causati nell'attività di acquisizione ed elaborazione di dati, nonché nella fornitura di *software* o sistemi completi. La garanzia opera specificamente in casi di divulgazione di informazioni, involontaria o per infedeltà dei dipendenti, e di danneggiamento, furto o incendio dei documenti e dei supporti consegnati dal cliente. Sono invece esclusi i danni agli impianti di elaborazione, le penalità contrattuali a carico dell'assicurato nella consegna di documenti o nell'elaborazione di dati, e i danni derivanti da difetto del materiale venduto o locato.

In Germania, infine, non esistono polizze concepite appositamente per le speciali esigenze delle *software houses*: di solito, offerte solo alcune garanzie per i danni patrimoniali, con esclusione dell'attività di consulenza e di programma-

zione, in forma di condizioni speciali elaborate caso per caso.

## 6. ASSICURAZIONE E TUTELA DELL'UTENTE

Pur nei limiti di questa panoramica parziale (che ha preso in considerazione solo gli aspetti inerenti al programma ed alla programmazione), appare evidente, come già si accennava in precedenza, che l'assicurazione rappresenta uno dei migliori mezzi di tutela attualmente a disposizione degli utenti informatici, soprattutto se di una certa dimensione economica.

Se, infatti, le analisi e gli studi condotti in campo giuridico mirano a far sì che nella fase di « patologia » dei negozi informatici il rischio (contrattuale e tecnologico) non resti per l'intero sul solo utente, da un punto di vista pratico le coperture assicurative possono concretamente dare attuazione, anche se non completa, a tale fine.

Ovviamente, un contratto di assicurazione non può e non deve sostituire quei doveri di informazione, collaborazione ed assistenza che le parti — e soprattutto il fornitore — devono osservare sia nella gestione del rapporto, sia nella fase prenegoziale. E d'altro canto, l'insufficienza o l'inadeguatezza delle coperture sul mercato — messa in rilievo in più punti — spesso evidenzia l'esistenza di lacune nell'area di tutela offerta all'utente. Tali considerazioni non intaccano però la sostanziale utilità di questo strumento, che permette un certo ristoro da quei danni altrimenti destinati a gravare su una sola parte, data l'onnipresenza di clausole di esonero da responsabilità nei contratti. La stessa difficoltà di definire ed imputare in molte ipotesi una precisa responsabilità, il non completo assestamento teorico della materia, il substrato scientifico, per nulla perfezionato, cui necessariamente si fa riferimento, sono elementi che rendono complessi i criteri di distribuzione del rischio tecnologico.

Un'assicurazione può avviare a molti problemi, soprattutto se stipulata e gestita avendo piena conoscenza delle potenzialità (anche nel rischio) del *computer* e dell'informatica.

SILVIA TRAVERSO