

RICERCHE

VERSO UNA POLIZZA ASSICURATIVA DEI RISCHI INFORMATICI

SOMMARIO

1. Premessa: prevenzione e assicurazione dei rischi informatici. — 2. L'ambito di operatività delle polizze elettroniche. — 3. Dalle polizze elettroniche alle polizze informatiche: la polizza « Tutti i rischi dell'informatica » delle Assicurazioni Generali. — 4. Due importanti clausole nella copertura *software*: la clausola riguardante le somme assicurate e quella riguardante il metodo di liquidazione dei sinistri. — 5. Altre garanzie: a) la copertura per le maggiori spese sostenute per la prosecuzione dell'attività; b) la copertura delle perdite patrimoniali derivanti da atti dolosi e fraudolenti.

1. PREMESSA: PREVENZIONE E ASSICURAZIONE DEI RISCHI INFORMATICI.

La diffusione dell'informatica ha fatto nascere una serie di nuovi problemi e rischi spesso non adeguatamente valutati¹. L'utente ha due possibilità contro il verificarsi di questi rischi: in primo luogo tentando di redigere contratti di compravendita, locazione e *leasing* del sistema elaborativo che siano i più equi possibile, ossia che tutelino lo stesso utente oltre che il solo costruttore come invece più spesso avviene². In secondo luogo sottoponendo gli impianti, i dati e i programmi ad una serie di misure di sicurezza fisica e logica.

Quando la prevenzione dei rischi non è sufficiente o non dà risultati, l'ultimo rimedio è l'assicurazione: con essa si limitano le conseguenze economiche di un sinistro o di un'illecita attività connessa con il *computer*.

In questa sede si focalizza l'attenzione sull'evoluzione delle polizze assicurative nella progressiva copertura di tutti i possibili rischi che possono colpire un cen-

tro EDP, curando in special modo le garanzie riguardanti il *software*, quelle riguardanti le maggiori spese sostenute dall'azienda per la prosecuzione dell'attività e infine quelle riguardanti le perdite patrimoniali derivanti da atti dolosi e fraudolenti.

¹ X. DATTIN nel suo articolo, *Come assicurare un CED*, in *Sistemi e automazione*, n. 224, marzo 1982, parla di una « seconda generazione » del rischio informatico caratterizzata da una parte dall'aggravarsi delle conseguenze dovute all'integrazione dell'informatica in tutto il sistema produttivo dell'impresa, dall'altra dall'ampliarsi dei tipi di rischio alle azioni di origine umana e dolosa, compresi il vandalismo, la distruzione volontaria, la frode.

² Questo perché i contratti sono spesso predisposti dal solo costruttore, che è di norma una grossa impresa, mentre l'utente può solo accettare o non accettare le condizioni e le clausole tutte del contratto stesso. Si veda a proposito G. ALPA, *I contratti di utilizzazione del computer*, in *Giur. it.*, 1983, IV, 42, pubblicato anche nel *Trattato Rescigno*, Torino, 1982.

Una chiara visione della progressiva crescita di complessità dei contratti informatici è offerta da E. BONAZZI, *Il sistema contrattuale dell'informatica*, in *Soc. dir.*, 1985, 49.

2. L'AMBITO DI OPERATIVITÀ DELLE POLIZZE ELETTRONICHE.

Le compagnie assicurative iniziarono ad offrire polizze specifiche nel settore

³ È ciò che si rileva dalla relazione di COPPOLA DI CANZANO sul tema *Esperienze internazionali in materia di rischi dell'informatica*, tenuta nel corso del terzo convegno Industria e assicurazione dal titolo « *Informatica e assicurazione* », svoltosi a Villa Manin di Passariano il 15 aprile 1983.

⁴ La polizza *all risks* è stata introdotta in Europa negli anni '70, beneficiando dell'esperienza già acquisita negli Stati Uniti da un gruppo di imprese assicuratrici americane come la St. Paul Fire and Marine Insurance, la New Hampshire Insurance Company, la Fireman's Fund.

⁵ Sulla differenza tra rischi diretti e indiretti e più in generale per una visione di insieme sui contratti assicurativi di base nel settore rischi informatici, vedi G.B. FORLINO, *Assicurazione e diritto informatico: i contratti assicurativi di base*, in *I contratti di informatica* (a cura di) G. ALPA-V. ZENO ZENOVICH, Milano, 1987, p. 361. Secondo la definizione dell'autore i rischi di natura diretta sono quelli in cui l'avvenimento considerato come potenzialmente dannoso consiste in un fatto accidentale e materiale che colpisce le attrezzature informatiche da un punto di vista fisico. I rischi di natura indiretta sono invece quelli nei quali l'avvenimento considerato come potenzialmente dannoso consiste in un fatto conseguente all'uso delle attrezzature informatiche che non sono più per sé considerate e che in sé possono anche non essere state fisicamente oggetto dell'avvenimento stesso.

⁶ Uno studio relativo ai costi del sistema informatico s'è contenuto nell'allegato ad *Espansione, Come assicurare i rischi nelle aziende*, n. 172, Mondadori, Milano, 1984, p. 117. I dati tecnici relativi ai costi del sistema informatico contenuti nel capitolo intitolato « *Garanzie per l'informatica* », possono dare un'idea su quali siano i rischi da coprire maggiormente oggi rispetto a ieri: nel 1970 le componenti principali di un sistema incidono sui costi in questo modo: il calcolatore e le unità periferiche per il 60%, le infrastrutture (cioè i locali ed i loro annessi) per il 10%, le risorse umane e il software per il 30%. Attualmente l'incidenza delle componenti è totalmente cambiata tanto che il calcolatore e le periferiche hanno una incidenza di costo del 20%, le infrastrutture anche del 20% mentre le risorse umane e il software hanno un peso del 60%. L'*hardware* non rappresenta più dunque il bene principale ma uno strumento di lavoro. La parte prevalente del patrimonio informatico è pertanto costituita dal software e dalle risorse umane.

⁷ Le polizze prese in esame per la redazione dello scritto sono quelle predisposte dalle seguenti compagnie: Assicurazioni Generali S.p.A., indicata con la lettera A; Ras, Riunione Adriatica di sicurtà, indicata con la lettera B; Assitalia S.p.A. del gruppo Ina, indicata con la lettera C; Guardian Royal Exchange Assurance, indicata con la lettera D; New Hampshire Insurance Company indicata con la lettera E; Lloyd Internazionale, indicata con la lettera F; Sai, Società Assicuratrice Industriale S.p.A., indicata con la lettera G; Toro Assicurazioni S.p.A., indicata con la lettera H; Ross Collins s.r.l., indicata con la lettera I. La polizza A, ad esempio, prevede 33 definizioni a cui le parti devono attribuire convenzionalmente il significato previsto dalla polizza stessa. La polizza C prevede, invece, solo 9 definizioni.

rischi informatici già una ventina di anni fa, stimolate forse anche dal fatto di essere esse stesse tra i maggiori utenti di sistemi EDP³. In quell'epoca le compagnie di assicurazione offrivano una copertura solo per la parte fisica degli elaboratori. Essa valeva contro tutti i rischi, meno quelli esplicitamente esclusi dalla polizza. Queste prime polizze elettroniche *all risks*⁴ permettevano di coprire i rischi corsi dall'*hardware* in caso di incendio, terremoto, acqua, cioè i c.d. rischi diretti all'*hardware*⁵.

La differenza fondamentale tra i contratti classici di assicurazione e i contratti *all risks* è che i primi necessitano di due definizioni importanti: 1) la definizione dei rischi coperti, per cui la garanzia dell'assicuratore è strettamente limitata alle cause di sinistro menzionate; 2) la definizione dei rischi esclusi che ha per fine, nell'ambito delle garanzie prestate, la limitazione delle garanzie stesse. I contratti *all risks*, invece, necessitano di una sola definizione, quella dei rischi esclusi, intendendo che ogni rischio non escluso è coperto senza che occorra una definizione più ampia. È evidente l'interesse per l'assicurato di una definizione di questo tipo: una dimenticanza avrà solo l'effetto di limitare le esclusioni e in tal caso, a seguito di un sinistro, è la compagnia di assicurazione a sopportarne le conseguenze.

Tuttavia l'evoluzione dell'informatica è caratterizzata dal crescente valore del software rispetto all'*hardware*⁶. Per fronteggiare le nuove esigenze il settore assicurativo ha dovuto modificare le modalità di approccio del rischio allargando la gamma delle garanzie offerte. Ne risultano contratti assicurativi non sempre intellegibili per l'utente. Non per niente molte polizze contengono una serie di definizioni che aiutano ad interpretare più facilmente il contratto stesso⁷.

In realtà, nella maggior parte dei casi, l'ambito di operatività delle polizze elettroniche è ancora limitato alla copertura dei danni materiali all'*hardware*, con tutt'al più l'offerta di due garanzie accessorie, intese l'una a risarcire le spese necessarie alla ricostituzione dei dati contenuti nei supporti danneggiati, l'altra a fornire copertura alle maggiori spese sostenute dall'azienda

per la prosecuzione dell'attività a seguito di un danno materiale al sistema elaborativo. Infatti la copertura *hardware*, cioè quella dei danni diretti al calcolatore, non presenta particolari problemi, trattandosi in sostanza di una normale assicurazione di cose nei confronti di normali eventi dannosi (ovviamente tenendo conto della particolare vulnerabilità del sistema elettronico nei confronti dei diversi rischi). Invece la copertura *software*, cioè la copertura delle spese per la ricostituzione dei dati, è molto più complessa. Il problema è di accertare l'effettivo contenuto dei nastri e dei dischi e di stabilirne un valore oggettivo. È per questo che, nella maggior parte dei casi, le compagnie di assicurazione tendono a coprire, oltre al costo materiale del supporto danneggiato, le sole spese per la reimmissione dei dati perduti partendo dagli originali, escludendo quindi il risarcimento di qualsiasi altro tipo di danno legato al valore delle informazioni, escludendo la perdita di dati senza che vi sia un danno fisico al supporto ed escludendo infine la perdita dei programmi⁸.

3. DALLE POLIZZE ELETTRONICHE ALLE POLIZZE INFORMATICHE: LA POLIZZA « TUTTI I RISCHI DELL'INFORMATICA » DELLE ASSICURAZIONI GENERALI.

Un passo avanti nella copertura *software* sarebbe dunque quello di offrire una copertura per la reintegrazione degli archivi (intendendosi per archivi sia i dati che i programmi) registrati sul supporto anche nel caso in cui non vi sia un danno fisico allo stesso.

Forse l'unica polizza in Italia che tende ad estendere la garanzia anche alla perdita o alterazione degli archivi senza danni materiali al supporto⁹ è la polizza « Tutti i rischi dell'informatica » delle Assicurazioni Generali (che d'ora in poi, come già stabilito, chiameremo polizza A). È questa una polizza caratterizzata dal fatto di essere concepita per dare copertura con un unico contratto all'intera casistica dei

rischi collegati ad un centro EDP. Essa prevede infatti i danni diretti all'*hardware* e al *software*, i danni indiretti conseguenti ad una interruzione di esercizio e alla responsabilità civile, i danni da impiego doloso del *computer*. La polizza A è un esempio di polizza informatica vera e propria, visto che la copertura si estende al *software* e ai rischi indiretti, non limitandosi alla parte visibile dell'elaboratore.

La polizza in esame prevede nella sottosezione A.2 denominata « Ricostituzione degli archivi »¹⁰, due punti molto interessanti. Il punto B dice: « La società si obbliga durante il periodo di efficacia della polizza a risarcire i costi

⁸ La polizza B ad esempio prevede in un'apposita appendice alla polizza base l'assicurazione dei supporti dei dati, con un preventivo questionario da sottoporre al cliente, ma all'art. 2 si precisa che la società non risponde dei costi derivati da: a) errata registrazione (errata programmazione, errata perforazione, errata iscrizione, errato inserimento); b) cancellature conseguenti ad errori di ogni genere; c) perdita di dati memorizzati causata dall'azione di campi magnetici. La polizza C in una clausola delle condizioni particolari prevede che la società indennizzi i costi necessari effettivamente sostenuti per il riacquisto dei supporti dati distrutti o sottratti nonché per la ricostituzione dei dati contenuti nei supporti stessi assicurati ma precisa che non sono indennizzabili i costi dovuti ad errata registrazione, a cancellazione per errore e a cestinatura per svista. Tali esclusioni sono previste esplicitamente anche dalle polizze E, F, H.

⁹ Secondo una ricerca di S. TRAVERSO, *Assicurazione e software*, in questa Rivista, 1986, p. 312, in Germania e in Francia esistono coperture in cui è previsto un caso di danno al *software* senza lesione al supporto: è l'ipotesi del fulmine, che provoca campi elettromagnetici in grado di smagnetizzare il dischetto. Anche in Gran Bretagna, secondo la stessa ricerca, alcune compagnie prevedono la copertura per la ricostituzione dei dati anche in caso di cancellazione accidentale. Tale garanzia però è concessa raramente, solo a clienti selezionati, con certi limiti di indennizzo, con determinate misure di sicurezza nel ricovero di dati e copie e con una franchigia pari a circa quattro ore di lavoro del *computer*.

¹⁰ La polizza definisce gli archivi come l'insieme dei dati e/o programmi di utente memorizzati sui supporti. Sempre tra le definizioni della polizza si legge per quanto riguarda i programmi di utente: « Sequenza di informazioni, che costituiscono istruzioni eseguibili dal calcolatore; che l'assicurato utilizza in quanto sviluppati per i suoi scopi da propri dipendenti, da società specializzate o prestatori d'opera da esso specificatamente incaricati ». I programmi di licenza d'uso si differenziano per essere una sequenza di informazioni che l'assicurato utilizza in base ad un contratto con il fornitore per fini e per un periodo di tempo limitati (uso temporaneo) o illimitati (uso permanente), specificati nel contratto stesso.

documentati sostenuti per la ricostituzione degli archivi (memorizzati sui supporti assicurati in sottosezione A.1) perduti o alterati per danno risarcibile alle cose assicurate in sottosezione A.1¹¹ o per difettoso funzionamento delle stesse dovuto a cause accidentali » (...). È appunto in quel « difettoso funzionamento delle stesse dovuto a cause accidentali » che, a mio avviso, possono senz'altro ricomprendersi i danni agli archivi senza danni al supporto.

Il punto C della stessa sottosezione dice: « La società si obbliga durante il periodo di efficacia della polizza a risarcire i costi documentati sostenuti per la ricostituzione e sistemazione degli archivi (memorizzati sui supporti assicurati in sottosezione A.1) perduti o alterati a causa di atti dolosi e fraudolenti di dipendenti o prestatori d'opera o di terzi; agli effetti della risarcibilità gli atti dolosi o fraudolenti devono essere commessi tramite: 1) alterazione del contenuto degli archivi effettuata direttamente o tramite le linee di trasmissione dati o tramite unità di *input* o tramite il trasporto di supporti tra i luoghi indicati in polizza; 2) furto o rapina di archivi; 3) progettazione o utilizzo diretto e determinante del sistema di elaborazione dati in maniera dolosa o fraudolenta; 4) utilizzo indebito di risorse elaborative e/o di potenza di calcolo ». In questo caso si coprono dunque anche gli interventi non autorizzati in cui vi è una perdita degli archivi ma senza necessariamente un danno anche ai supporti.

Abbiamo detto che la garanzia per la ricostituzione degli archivi contemplata dalla polizza in esame, implica tanto la copertura per la perdita dei dati quanto la copertura per la perdita di programmi di utente¹². Ma mentre per la perdita dei dati è possibile, sia pure con una

certa approssimazione, quantificare i costi da parte dell'assicuratore, valendosi di statistiche con cui fissare il livello medio dei costi che un centro per la ricerca di informazioni sostiene per la loro codifica ed immissione, per la perdita dei programmi è impossibile procedere allo stesso modo. Occorrerebbe da parte dell'assicuratore conoscere il livello medio di aggiornamento e di manutenzione del programma come pure la sua utilità e le eventuali disfunzioni. La copertura per la perdita di programmi può dunque trasformarsi in un'occasione di illecito arricchimento venendo ad addebitare all'assicuratore costi che non gli competono. È per questo che la polizza A pone dei presupposti a condizione delle garanzie specifiche per la ricostituzione degli archivi: a) anzitutto l'assicurato deve conservare copie di sicurezza degli archivi di proprietà sua e dei clienti; b) l'accesso agli archivi, ai programmi in licenza d'uso e alle cose assicurate in sottosezione A.1 deve essere consentito solo a personale autorizzato dipendente o prestatore d'opera; c) la società non è obbligata per i danni effettuati da dipendenti o prestatori d'opera già condannati per atti dolosi o fraudolenti e del cui fatto l'assicurato era o poteva essere a conoscenza; d) il sistema di elaborazione dati deve essere dotato di *software*, indicato nel prospetto di polizza, che fornisca la documentazione dei processi elaborativi svolti, finalizzata a dimostrare la successione degli eventi che hanno causato il danno (in questo modo si ovvia all'impossibilità dell'assicuratore di accertare il danno); e) il trasporto degli archivi deve essere effettuato da dipendenti dell'assicurato o da ditte specializzate nel trasporto di materiale informatico e assicurate con adeguata copertura trasporti; f) il trasporto delle copie di sicurezza deve essere effettuato mantenendo sempre nel locale di partenza almeno la copia di sicurezza precedente. Inoltre la struttura generale della polizza A rimane di tipo *all risks* ma nel caso riguardante appunto la copertura del *software*, vengono indicati minuziosamente i casi in cui la società assicuratrice si obbliga al risarcimento. Infine il risarcimento è limitato per quanto riguarda i dati, ai costi necessari e documentati sostenuti

¹¹ La sottosezione A.1 prevede il risarcimento danni materiali e diretti degli apparecchi ed impianti, dei programmi in licenza d'uso, dei supporti e di quant'altro indicato nel prospetto di polizza.

¹² La ricerca già citata in nota 9 di S. TRAVERSO, *Assicurazione e software* menziona altri due casi in cui viene risarcita la perdita del programma: la polizza giapponese e quella inglese.

dall'assicurato per la ricerca, il recupero e le reimmersione dei dati perduti a partire dall'ultima copia di sicurezza, per quanto riguarda i programmi di utente, ai costi necessari e documentati sostenuti dall'assicurato per la ricerca del danno e il ripristino dei programmi stessi perduti fino all'ultimo stadio di modifica degli stessi e calcolato secondo i costi di reimmersione a partire dalla copia di sicurezza.

4. DUE IMPORTANTI

CLAUSOLE NELLA COPERTURA SOFTWARE:

LA CLAUSOLA

RIGUARDANTE LE SOMME ASSICURATE E QUELLA RIGUARDANTE IL METODO DI LIQUIDAZIONE DEI SINISTRI.

La determinazione della somma assicurata è dunque una clausola particolarmente importante nell'ambito della copertura *software*¹³.

L'assicurazione, in questo caso, è prestata a primo rischio assoluto ossia la compagnia assicuratrice si assumerà dietro giustificativo le spese di ricostituzione delle informazioni perdute e dei supporti danneggiati, ma solo fino alla concorrenza del capitale assicurato. L'assicurato determinando il valore per cui richiede la copertura è dunque responsabile della qualità della copertura stessa: ogni ottimismo nella valutazione si traduce in una copertura insufficiente¹⁴.

È importante un'esatta valutazione dei costi necessari per la ricostituzione dei dati. A questo proposito esistono vari sistemi che gli assicuratori adottano normalmente d'accordo con l'assicurato¹⁵. Uno di questi consiste nell'effettuare una suddivisione analitica del patrimonio informatico distinguendo i supporti cartacei, i nastri, i dischi ed eventualmente altri, secondo l'importanza e la densità delle informazioni contenute. Ad ognuna di queste classi e per ogni tipo di supporto si cerca di attribuire il valore, che il capocentro stima essere il più corretto, ovviamente integrato dal costo di riacquisto del supporto¹⁶.

Ai fini del sistema tariffario, una volta determinata la somma assicurata, il tecnico della società assicuratrice dovrà valutare le caratteristiche oggettive del rischio, quindi prendere visione delle prevenzioni generali adottate dall'assicurato, constatare l'organizzazione del centro, le misure di soccorso e di salvataggio, le modalità di conservazione dei supporti, la regolarità dei controlli di manutenzione e così via¹⁷.

Il metodo di liquidazione dei sinistri prevede alcuni punti validi generalmente: 1) anzitutto l'assicurato è tenuto, in seguito ad un sinistro e nel caso vi siano supporti deteriorati, a dimostrarne l'esistenza; 2) ogni indennizzo è corrisposto all'assicurato solo dopo l'avvenuta ricostruzione dei dati memorizzati sui supporti; 3) il periodo massimo in cui può avvenire la reintegrazione e il ripristino è per lo più di un anno, dopo tale periodo i costi di reintegrazione non sono coperti.

Il pagamento dell'indennizzo viene inoltre effettuato previa detrazione di una franchigia a carico dell'assicurato.

¹³ Nel caso di copertura danni diretti all'*hardware*, la somma assicurata deve essere uguale al costo di rimpiazzo a nuovo, ossia al prezzo di listino, comprensivo delle spese di trasporto, dogana e montaggio di un apparecchio o impianto nuovo, uguale o equivalente per caratteristiche, prestazioni e rendimento. Se la somma assicurata risulta inferiore al costo di rimpiazzo a nuovo al momento del sinistro, l'indennità è ridotta in proporzione al rapporto tra valore assicurato e valore assicurabile (c.d. regola proporzionale art. 1907 c.c.). Questa clausola è valida generalmente per tutte le polizze analizzate in questa ricerca.

¹⁴ La polizza B, nell'appendice riguardante i supporti dati, prevede all'art. 3 (denominato somma assicurata) che: « la somma assicurata di L. ... dovrà corrispondere ai costi necessari per il riacquisto di tutti i supporti dati assicurati e per la ricostituzione delle informazioni in esse contenute. Detta somma rappresenta il limite massimo di indennizzo ».

¹⁵ Una esauriente trattazione dei sistemi di valutazione dei costi è contenuta negli studi del convegno *Informatica e assicurazione*, cit., pp. 184-185.

¹⁶ Qualcosa del genere avviene per esempio, nelle clausole della polizza B valide per l'inclusione delle memorie esterne nella polizza base.

¹⁷ Contratti di manutenzione sono previsti da praticamente tutte le polizze elettroniche da me esaminate. Sulla manutenzione del *software* si veda ROSSELLO, *I contratti di manutenzione del software*, in G. ALPA-V. ZENO ZENCOVICH (a cura di), *I contratti di informatica*, cit., p. 203.

**5. ALTRE GARANZIE: A) LA
COPERTURA PER LE
MAGGIORI SPESE SOSTENUTE
PER LA PROSECUZIONE
DELL'ATTIVITÀ; B) LA
COPERTURA DELLE PERDITE
PATRIMONIALI DERIVANTI
DA ATTI DOLOSI
E FRAUDOLENTI.**

Tra le estensioni di garanzia previste dalle polizze oggi in vigore sul mercato italiano vi sono anche una serie di clausole destinate alla copertura dei danni c.d. indiretti, quali ad esempio le maggiori spese sostenute dall'azienda per la prosecuzione dell'attività a seguito di un danno materiale al sistema elaborativo (es. spese di personale, noleggio di un calcolatore sussidiario, affitto di locali ecc.). Un'altra serie di clausole è diretta alla copertura delle perdite patrimoniali derivanti da atti dolosi o fraudolenti, ossia dai c.d. *computer crimes*.

a) L'azienda, nell'ipotesi di un blocco nel funzionamento dell'elaboratore, può risentire di pesanti ripercussioni sulla sua attività o addirittura essere costretta alla chiusura. Uno studio condotto negli USA dall'Università del Minnesota, ha calcolato che per un'impresa industriale con un fatturato di 250 miliardi di lire un'interruzione del sistema informativo provoca danni per 35 milioni di lire al giorno nella prima settimana, 1 miliardo di lire al giorno nella seconda, 3 miliardi alla fine della terza e può risultare fatale per l'impresa medesima se il sistema informativo non viene rimesso in efficienza entro la quarta settimana¹⁸.

È necessario pertanto predisporre un programma di emergenza determinando sistemi di riserva già quando il sistema elaborativo parte e non dopo avvenuto il sinistro, per non rischiare di allungare considerevolmente il periodo di mancata elaborazione.

Il primo problema è quindi quello di verificare quali possibilità vi siano di proseguire l'attività se un grave danno dovesse colpire il sistema elaborativo. Il secondo problema è quello di valutare i costi e di verificare l'idoneità del sistema di riserva.

Negli atti del convegno tra industria e assicurazioni sui rischi dell'informatica già citato, sono analizzati vari tipi di soluzione al primo dei problemi accennati. Poche di esse sono però effettivamente praticabili. Ecco le possibili soluzioni proposte: 1) Manualizzazione delle procedure. È l'ipotesi meno praticabile perché richiede un'accurata documentazione di tutto l'elaborato, risorse notevoli di macchine e uomini, senza contare la difficoltà della riconversione. 2) Ricerca di altro macchinario. È un'altra soluzione difficilmente praticabile in quanto richiederebbe accordi precisi con il fornitore affinché fosse sempre disponibile un intero parco macchine a magazzino. 3) *Hardware* in deposito. È un'ipotesi più concreta ma comunque estremamente costosa: infatti l'azienda dovrebbe comunque sobbarcarsi un forte stanziamento improduttivo e crescere nel tempo, per tenere il deposito sempre in linea con l'evoluzione fisica del centro. 4) Accordi tra due o più aziende. È una strategia praticabile ma che richiede la sicurezza di una completa compatibilità dei centri e prove periodiche sulla fattibilità del soccorso. 5) Raddoppio del centro. È una soluzione buona ma praticabile solo da aziende di grandi possibilità finanziarie. 6) Centro di continuità e servizio. È una soluzione nata negli Stati Uniti e che ora sta affacciandosi in Europa. Si tratta di centri di grandi capacità elaborative al servizio di un esiguo numero di abbonati per le loro necessità generali ma soprattutto in occasione di eventuali disastri.

La soluzione dei centri di continuità, accennata al punto 6 sopra citato, può rappresentare una tra le più valide proprio se nasce da un accordo tra utilizzatori, costruttori e assicuratori. Un « contratto di soccorso » di questo genere offre all'azienda le seguenti prestazioni: 1) copertura assicurativa per tutti i macchinari; 2) disponibilità del centro di soccorso, qualora avvenga un danno risarcibile, per tutta la durata necessaria alla rimessa in funzione del centro sini-

¹⁸ MARIO G. LOSANO, *Il diritto privato dell'informatica. Corso di informatica giuridica*, Torino, 1986, p. 144.

strato; 3) verifica e controllo periodico della compatibilità del centro di soccorso con il centro dell'utilizzatore; 4) copertura delle spese incontrate per eventuale perdita di supporti e delle informazioni ivi contenute; 5) copertura di tutte le altre spese sostenute per la prosecuzione dell'esercizio in aggiunta a quelle relative al centro di soccorso; 6) possibilità di utilizzare il centro di continuità anche per le altre necessità improvvise che non siano a seguito di sinistro indennizzabile.

Un tale accordo limitato a circa 50 utenti, dà all'azienda una sufficiente sicurezza di prosecuzione dell'esercizio considerato anche che il centro può essere utilizzato entro 24 ore dal sinistro. In Francia un tale esperimento ha già avuto attuazione, mentre in Italia è stato solo annunciato senza avere peraltro seguito concreto. Pur non essendo ancora applicato il contratto di soccorso, in Italia è prevista comunque nelle normali polizze elettroniche una copertura assicurativa per i maggiori costi per la prosecuzione dell'esercizio¹⁹.

Il termine « maggiori spese » richiede una precisazione: esso sottintende che dai costi sostenuti per la prosecuzione dell'attività occorrerà detrarre quelli che sarebbero stati comunque sopportati per le medesime elaborazioni se non fosse accaduto il sinistro, questo evidentemente perché l'assicurato non deve beneficiare o trarre profitto dal sinistro.

La somma assicurata nel caso di questa garanzia è, in tutta Europa, riferita ai costi sostenuti su base annua a fronte di determinate voci che l'utente intende assicurare²⁰.

Anche per questa garanzia sono previste misure di cointeressamento dell'assicurato nel danno, quali franchigie o scoperti in percentuale del danno²¹.

b) Secondo ricerche condotte dalla *Union Leader* nel 1981, in USA ogni frode attuata per mezzo del computer provoca un danno medio di mezzo milione di dollari: si tratta quindi di un danno medio notevolmente più elevato che per le rapine generiche (3.200 dollari) e per le rapine alle banche (23.500 dollari). Questi dati tuttavia hanno una rilevanza solo marginale visto che si tratta di avvenimenti di cui è difficile delineare gli esatti contorni sia per l'o-

biettiva difficoltà di determinare talvolta le conseguenze economiche che ne derivano, sia per l'estrema ma comprensibile ritrosia degli interessati a pubblicizzare circostanze inerenti alla propria attività (si pensi alle banche).

La maggior parte dei comportamenti fraudolenti fino ad oggi scoperti (e resi noti) indirizzati verso sistemi informativi dalle aziende utilizzatrici, appaiono costituiti da manipolazioni dei processi di elaborazione elettronica.

Vi sono tre fasi del processo elaborativo dati in cui le manipolazioni possono essere attuate: 1) la fase di immissione dati (*input*); 2) la fase di elaborazione dati (in questo ambito si distinguono le c.d. manipolazioni di programma dalle manipolazioni c.d. di *console*); 3) la fase di emissione dati (*output*).

La maggiore pericolosità delle manipolazioni di *input* e di programma deriva dal fatto che le stesse, una volta impostate con successo, sono estremamente difficili da scoprire sia perché vengono praticamente gestite automaticamente dal computer, ripetendosi nel tempo senza alcun intervento diretto da parte dell'autore, sia perché l'autore stesso è in grado di programmare l'autocancellazione delle manipolazioni effettuate e quindi di non lasciare traccia delle operazioni illecite compiute.

Le manipolazioni dell'*input* presuppongono l'esistenza di un elaboratore

¹⁹ L'appendice alla polizza B per esempio estende l'assicurazione alle spese supplementari costituite da: « a) spese di utilizzazione di un altro sistema di elaborazione dati in sostituzione di quello assicurato parzialmente o totalmente danneggiato; b) spese di personale per l'utilizzazione di tale sistema sostitutivo ». Così pure le polizze A, C, E, F prevedono nelle condizioni particolari, valide cioè solo se espressamente richiamate, delle clausole per la copertura dei maggiori costi. Negli atti del convegno *Informatica e assicurazioni* già citato sono riportati in dettaglio le principali componenti che normalmente vengono considerate maggiori spese.

²⁰ La clausola B.4 della polizza A prevede, ad esempio, che: « La somma assicurata deve essere pari ai costi di esercizio aggiuntivi previsti su base annua per la prosecuzione della medesima attività dichiarata, determinati conteggiando i costi mensili che si intendono come limite massimo di risarcimento per mese ».

²¹ Ad esempio nella clausola A comma 6 delle condizioni particolari polizza C.

già programmato e si realizzano semplicemente inserendovi dati falsi o informazioni corrette in momenti sbagliati, al fine di sfruttare l'elaborazione secondo programma di tali *input* manipolati²².

Nell'ambito delle manipolazioni in fase di elaborazione dati, quelle c.d. di programma, come già si è detto, risultano essere le più insidiose. Le tecniche seguite sono numerosissime²³ e assumono nella letteratura nord-americana bizzarri nomi come « il cavallo di Troia » che consiste nel piazzamento segreto di istruzioni nel programma in modo tale da far svolgere all'elaboratore delle funzioni non autorizzate, permettendogli però anche di continuare a svolgere le sue normali funzioni come « la tecnica del salame » che consente l'appropriazione di piccoli quantitativi di beni da un gran numero di riserve da accreditare poi tutti su un solo conto.

Nell'assenza di norme specifiche contro la criminalità informatica, soprattutto nel settore bancario dove più che in altri settori in Italia si è manifestata la vulnerabilità dei sistemi elettronici di elaborazione dei dati, i contratti assicurativi possono aiutare a combattere quello che rischia di divenire un vero e proprio flagello sociale²⁴. L'ambito di copertura in esame è però ancora tutto da esplorare, a meno che non si voglia non offrire garanzie come quelle recepite dal mercato austriaco, che coprono la frode informatica limitandola però a massimali dell'ordine della decina di milioni di lire²⁵.

²² Un esempio tipico riguarda le ipotesi di truffa al sistema Bancomat realizzate in Italia inserendo semplicemente negli sportelli automatici dati relativi ad un cliente vero ma abusivamente riprodotti su esemplari non autentici di tessere o carte a banda magnetica, così da ottenere la consegna secondo programma delle somme di danaro richieste.

²³ Il *Criminal Justice Resource manual* a cura dell'U.S. Department of Justice, riporta una lunga serie di modi operandi rilevati nella commissione di *computer crimes*.

²⁴ In Italia la polizza della compagnia I (così come risulta anche dalla ricerca di F. STORACE, *La copertura assicurativa del rischio informatico*, in questa Rivista, 1986, 652) prevede una copertura per le frodi derivanti dall'uso di *computer* con riferimento particolare al settore finanziario e bancario.

²⁵ E. GRIMALDI, *Che fine ha fatto la polizza elettronica?*, in *Giornale delle assicurazioni*, n. 67, maggio 1986.

È ovvio invece che, per loro natura, i rischi ingenerati da questo tipo di azioni fraudolente sono di ordini di grandezza molto superiori. Ma non è facile trovare assicuratori disposti ad esporsi in un campo ancora così incerto. Gli stessi Lloyds di Londra hanno lanciato uno schema di polizza già nel 1981, ma si sono presto accorti di non poter affrontare un mercato ancora poco noto con un questionario strutturato su centinaia di domande di difficile compilazione e di dubbia utilità.

In Italia, la polizza della compagnia A prevede nella sezione D (denominata « Perdite patrimoniali da atti dolosi o fraudolenti ») una copertura piuttosto efficace ed estesa per una serie di rischi: perdita di valori, azioni, monete, titoli e simili, impianti, merci, materie prime, prodotti semilavorati e finiti o in corso di lavorazione, furto e copiatura di archivi e programmi in licenza d'uso specificatamente designati, utilizzo indebito di risorse elaborative e/o potenza di calcolo, perdita di profitto lordo.

Anche qui, come nel caso della copertura delle spese per la ricostituzione degli archivi, la condizione di garanzia (e la misura precauzionale) principale è la precisa documentazione dei processi elaborativi svolti, effettuata tramite un *software* di cui deve essere dotato il sistema elettronico di elaborazione assicurato. Questa documentazione deve dimostrare la successione degli eventi che hanno causato il danno.

Accanto a questa clausola ve ne sono però molte altre: « a) che l'assicurato all'atto della sottoscrizione della polizza non sia a conoscenza di alcun fatto doloso o fraudolento effettuato o tentato contro di lui, anche se non risarcibile dalla polizza. Egli inoltre deve obbligarsi a notificare tutti i fatti o tentativi di dolo o frode commessi da chiunque durante l'efficacia della garanzia anche se non risarcibili dalla polizza; b) che l'assunzione e il controllo del personale sia effettuato, nei limiti concessi dalla legge, con la massima scrupolosità; c) che tutti i controlli esterni e interni, le procedure di sicurezza fisica e logica, le misure di riconoscimento e di controllo, indicati dall'assicurato all'atto della sottoscrizione della polizza, siano mantenuti in vigore e in perfetta efficienza per tutta la durata della polizza; inoltre tali mi-

sure siano controllate nella loro efficacia con la cadenza fissata in polizza e ne sia mantenuto il verbale con la registrazione; d) che l'assicurato non porti a conoscenza nessuna persona, con l'eccezione delle persone che ne hanno diritto, dell'esistenza della garanzia. Qualora non siano rispettati questi presupposti, vale il dispositivo degli artt. 1892, 1893, 1989 cod. civ. ».

Un'ultima condizione, considerata come essenziale dalla polizza stessa ma, a mio parere, molto onerosa per l'assicurato, è che il meccanismo e le modalità del fatto criminoso devono essere conosciute e provate all'assicurato stesso e che il fatto e il colpevole devono essere denunciati all'autorità di polizia. Sappiamo infatti quanto sia difficile, in casi di questo genere, risalire al colpevole di un'azione fraudolenta ai danni di un sistema di elaborazione dei dati.

La polizza prevede inoltre delle limitazioni della copertura assicurativa di natura generale, temporale e territoriale. Le più interessanti sono senz'altro le prime. La clausola D.3 dice: « La società non è obbligata per: a) danni risultanti dall'introduzione nel sistema informativo dell'assicurato di documenti precedentemente falsificati »; quindi per la maggior parte dei furti effettuati per esempio attraverso il sistema Bancomat non vi può essere una copertura mediante questo tipo di polizza; b) danni dovuti ad investimenti non eseguiti, perdita di immagine o fiducia, perdita di utili sperati e perdite derivanti da sparizioni inesplicabili; c) danni causati da dirigenti di società le quali siano qualificabili come controllanti, controllate o collegate o affiliate ».

Le numerose condizioni e limitazioni della garanzia in esame dimostrano come, in materia di garanzia per perdite derivanti da atti dolosi o fraudolenti, vi siano ancora molte paure e titubanze da parte delle compagnie assicuratrici. Questa incertezza deriva anche dalla mancanza di una normativa che eviti pericolose lacune nell'ordinamento ancora sfornito di rimedi specifici.

Un esempio valga per tutti: una sentenza del Tribunale di Torino del 12 dicembre 1983 esaminando una fattispecie concernente un programma redatto da un'impresa, sottratto da un

dipendente di quest'ultima e riprodotto su un altro supporto, ha escluso che il fatto potesse essere perseguito come furto non trattandosi di cosa mobile ai sensi dell'art. 624 cod. pen.²⁶.

EUGENIO NASTRI

²⁶ Trib. Torino 12 dicembre 1983, in *Giur. it.*, 1984, II, 351.