

**CONVEGNO ORDINE INGEGNERI DI MILANO  
CEFRIEL - CLUSIT – CISCO**

**“LA SICUREZZA DELLE RETI”**

---

**TUTELA E SICUREZZA DEI DATI PERSONALI:  
LE RESPONSABILITA' CIVILI**

**MILANO, 8 APRILE 2003**

**EMILIO TOSI**

Ricercatore  
Istituto di Diritto Privato dell'Economia  
Università di Milano-Bicocca

Docente di Diritto Privato dell'Informatica e di Internet  
Master in “Diritto delle Comunicazioni”  
Università di Milano

Avvocato in Milano ([info@tosilex.com](mailto:info@tosilex.com))

## **1 - La tutela dei dati personali in Internet**

La diffusione globale *dell'e-commerce* - all'origine del fenomeno della commercializzazione della rete Internet - è conseguenza della progressiva diffusione della piattaforma di comunicazione tecnologica ipertestuale e *user friendly* denominata *world wide web* (www).

L'affermazione del commercio elettronico su larga scala ha posto - *ex multis* - il problema, particolarmente delicato ed attuale, della tutela dei dati personali online, raccolti mediante Internet quindi, con particolare riferimento ai dati trattati nell'ambito di attività di commercio elettronico e di *e-business* in senso ampio.

Si pensi alle problematiche generali connesse alla raccolta visibile di dati *online* e a quelle specifiche relative alla raccolta invisibile dei dati mediante utilizzo di registri elettronici - c.d. *data log* - per controllare gli utilizzatori di Internet e di dispositivi software - c.d. *cookie* - in grado di ricostruire accuratamente i comportamenti consumeristici - e non - dell'utilizzatore (c.d. "profilazione").

In senso favorevole all'applicabilità a Internet e al Commercio elettronico della Direttiva comunitaria 24 ottobre 1995, n. 46 — relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali — e della Direttiva comunitaria 15 dicembre 1997, n. 66 (che dovrà essere sostituita dalla recente Direttiva CE 12 luglio 2002, n.58 entro il 31 ottobre 2003)— relativa alla tutela della vita privata nel settore delle telecomunicazioni — si è espresso anche il *Gruppo di lavoro per la tutela delle persone con riguardo al*

*trattamento dei dati personali* — istituito dall'art. 29 della Direttiva 95/46 —  
rilevando che:

*“Sotto il profilo giuridico Internet non opera nel vuoto: il trattamento dei dati personali su Internet deve pertanto rispettare i principi della tutela dei dati così come avviene al di fuori della rete. Ciò non limita assolutamente il ricorso ad Internet, ma al contrario fa parte degli elementi fondamentali volti ad assicurare la fiducia degli utenti nel funzionamento di Internet e dei servizi forniti da esso. La tutela dei dati su Internet è quindi una condizione indispensabile per l'accettazione del commercio elettronico”.*

Da ultimo la Raccomandazione del Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali n.2/01 – *Requisiti minimi per la raccolta di dati online nell'Unione Europea* - del 17 maggio 2001, ha dato attuazione al principio di applicabilità della richiamata normativa comunitaria vigente, anche a Internet e al commercio elettronico, precisando una serie di requisiti minimi da soddisfare per la raccolta di dati personali online e precisamente stabilendo:

- obblighi informativi minimi a favore dell'interessato dal trattamento, in buona sostanza attuativi delle disposizioni delle Direttive CE citate (identità, indirizzo fisico e elettronico del titolare/responsabile del trattamento; finalità del trattamento; natura facoltativa o obbligatoria delle informazioni richieste; modalità del trattamento, evidenziando l'eventuale raccolta automatica di dati personali; misure di sicurezza adottate e durata del trattamento; diritti dell'interessato; ambito di comunicazione dei dati e così via);

- modalità "trasparente" di presentazione online delle informazioni predette: le informazioni devono essere fornite interattivamente e apparire sullo schermo del computer dell'interessato.

La prassi del commercio elettronico è, senza dubbio, caratterizzata da numerose occasioni di raccolta dei dati personali del navigatore - consumatore "virtuale", ora palesi - mediante la richiesta di compilazione di generici formulari elettronici o di veri e propri ordini di beni o servizi - ora occulte - si pensi al caso emblematico della raccolta automatica di dati personali mediante i c.d. *cookie* di cui si dirà *amplius* successivamente.

E', quindi, ormai dato incontestabile che anche la raccolta e il trattamento dei dati personali via Internet debbano, quindi, essere improntati al rispetto dei principi generali indicati dalla L. 675/96.

In particolare sembra opportuno richiamare i seguenti principi generali:

- il *principio di liceità e trasparenza* del trattamento dei dati personali posto dall'art.9;
- il *principio dell'informativa* all'interessato posto dall'art.10;
- il *principio del consenso* dell'interessato posto dall'art.11;
- il *principio della notificazione* al Garante del trattamento di dati personali da parte del titolare posto dall'art.7;
- il *principio di sicurezza* del trattamento posto dall'art. 15.

Le norme richiamate - come già si è detto in relazione al problema del controllo degli utenti - costituiscono un importante parametro di valutazione della liceità del trattamento dei dati personali su Internet e nel commercio elettronico.

L'art.9 della L.675/96 è di fondamentale importanza perchè fornisce all'interprete i criteri generali di valutazione della liceità del trattamento, utili anche ai fini dell'azione risarcitoria di cui all'art.18 per il caso di danni derivanti da trattamento illecito.

In particolare detto articolo stabilisce che i dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;

c) esatti e se necessario aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per cui sono raccolti o successivamente trattati;

d) conservati come dati personali per un periodo non superiore a quello necessario per le finalità per cui sono stati raccolti o successivamente trattati.

Occorre, infine, chiarire che cosa s'intenda per *dato personale e trattamento*

Per *dato personale* l'art. 1.2, lett. c) della L. 675/96, stabilisce che si deve intendere: "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale".

Per *trattamento* l'art. 1.2, lett. b) della L. 675/96, precisa che si deve intendere "qualunque operazione o complesso di operazioni (...) concernenti la

raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati".

## 2 – Il principio di sicurezza

Ma veniamo ora al *principio di sicurezza*. La mancata osservanza di misure di sicurezza necessarie alla sicurezza dei dati costituisce trattamento illecito sanzionato sia dal punto di vista civile che da quello penale (art. 36 L. 675/96).

L'*Internet Service Provider* – e più in generale qualsiasi soggetto che effettui trattamento di dati personali - deve in base alla legge citata adottare una serie di misure sia tecniche che organizzative atte a garantire la sicurezza dei dati personali trattati.

L'art. 15 L. 675/96 stabilisce che:

*"I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*.

L'omessa adozione di misure preventive di sicurezza è - si ribadisce - un fatto rilevante sia dal punto di vista civile che da quello penale.

Sotto il profilo civile il titolare ed il responsabile del sistema informatico connesso alla rete utilizzato per fornire servizi di accesso a Internet in caso di omessa adozione delle misure preventive di sicurezza sono tenuti al risarcimento dei danni causati dal trattamento, sia di quelli relativi al difetto di *sicurezza nel sistema che al difetto di sicurezza del sistema*.

L'omessa adozione di sistemi antivirus e di *firewall* a tutela degli accessi ai *server* del sistema informatico del *service provider* costituiscono senza dubbio fatti rilevanti sotto il profilo della risarcibilita` di eventuali danni conseguenti alle predette omissioni.

L'omessa adozione - da parte del titolare e del responsabile - di misure preventive di sicurezza rientrando nel concetto di trattamento non corretto ex art. 9, comma 1, lett. a) comporta oltre al risarcimento del danno patrimoniale anche di quello non patrimoniale per espressa disposizione dell'art. 29, comma 9 L. 675/96.

La legge all'art. 15, comma 2 prevede che con specifico regolamento vengano regolate - tempo per tempo - le misure minime preventive di sicurezza da adottare per il trattamento corretto dei dati personali.

Il criterio di idoneita` e adeguatezza adottato dal legislatore e` di indubbia relativita` e variera` in relazione allo stato della tecnica, alla natura dei dati trattati e alle specifiche caratteristiche del trattamento.

Il soggetto danneggiato, in forza del richiamo espresso dell'art. 18 L. 675/96 all'art. 2050 c.c., dovrà semplicemente dimostrare il fatto storico - l'evento dannoso e il rapporto causale tra fatto e danno - mentre al danneggiante spetterà la prova liberatoria - senza dubbio impegnativa - consistente nel dimostrare di aver adottato ogni possibile cautela per evitare il danno non essendo sufficiente dimostrare di non aver violato norme di legge o di prudenza e perizia.

Il titolare del trattamento nel caso in cui l'inosservanza delle norme di sicurezza determini un danno puo` sottrarsi alla relativa responsabilita`

civile non tanto provando di aver osservato le prescrizioni "minime" - che serve solo ad escludere la *responsabilita` penale ex art. 36 L. cit.* - quanto se dimostra di aver adottato *tutte* le misure idonee ad evitare il danno.

### **3 – Le responsabilità civili**

Trattasi - essenzialmente - delle responsabilità connesse al trattamento illecito dei dati personali e all'inosservanza delle misure necessarie alla sicurezza dei dati: ipotesi sanzionate anche penalmente dagli artt. 35 e 36 della L. 675/96.

Si osservi che l'art.18 L.675/96, stabilisce che:

*"chiunque cagiona danno ad altri per effetto del trattamento di dati personali e` tenuto al risarcimento del danno ai sensi dell'art. 2050 del codice civile".*

In base all'art. 2050 c.c..

*"Chiunque cagioni danno ad altri nello svolgimento di un'attività` pericolosa (...) e` tenuto al risarcimento del danno, se non prova di aver adottato tutte le misure idonee ad evitare il danno".*

L'importante conseguenza di tale previsione normativa e`, quindi, l'equiparazione dell'esercizio di attività` di trattamento dei dati personali all'esercizio di attività` pericolose per le quali l'art. 2050 c.c. prevede - come sopra visto - un alleggerimento significativo dell'onere della prova a carico del danneggiato rispetto alla regola generale di cui all'art. 2043 c.c.: onere del danneggiato sara`, infatti, solo quello di provare il danno e il rapporto di causalita` tra fatto e danno (e non anche il dolo o la colpa dell'autore del fatto illecito), mentre incombera` al danneggiante l'onere - ben piu` impegnativo - di provare di aver posto in essere tutte le misure idonee per evitare l'evento dannoso non essendo sufficiente dimostrare di non aver violato norme di legge

o di prudenza e perizia.

Mentre incombe al danneggiato dimostrare la sussistenza del nesso di causalità al danneggiante incombe l'onere di provare l'adozione di tutte le misure idonee ad evitare il danno.

Per misure idonee ad evitare il danno devono intendersi tutti gli accorgimenti previsti da norme legislative o regolamentari che disciplinano la specifica attività interessata dalla controversia: nel caso specifico non solo alle norme della L. 675/96, al regolamento tecnico in materia di misure minime di sicurezza previste dall'art. 15.2, ma anche alle prescrizioni impartite dal Garante o i *codici di deontologia e di buona condotta*.

Il richiamo all'art. 2050 c.c. non rende necessario appurare nel caso concreto se il trattamento sia pericoloso "per sua natura o per la natura dei mezzi adoperati", avendo il semplice effetto di chiarire la responsabilità del soggetto operante il trattamento in difetto della prova liberatoria anzidetta.

È il legislatore ad aver valutato preventivamente la pericolosità dell'attività del trattamento dei dati personali: la rilevanza sociale di tale attività ha condizionato la scelta normativa. Evidentemente la pericolosità si riferisce - in questo specifico contesto - non tanto al pericolo di incolumità fisica degli individui - che peraltro non può essere esclusa in assoluto - quanto alla potenziale lesività connessa al trattamento di dati relativi alla personalità dell'individuo. Pericolosità che risulta ancora maggiore quando il trattamento avvenga *online* tenuto conto dell'amplificazione che la rete Internet può dare a trattamenti illeciti.

L'art. 9 (*Modalità di raccolta e requisiti dei dati personali*) della L. 675/96,

come si è già rilevato, stabilisce le modalità del trattamento.

L'art. 15 (Sicurezza dei dati) della L. 675/96 prevede l'obbligatoria adozione di misure atte a garantire la sicurezza del trattamento.

Gli artt. 9 e 15 della L. 675/96 indicano a quali condizioni possa essere considerato lecito il trattamento anche su Internet

La sola violazione delle prescritte modalità di raccolta ovvero dei requisiti qualitativi dei dati personali - pur non essendo sanzionata né penalmente né amministrativamente - legittima colui che ha subito un danno a causa di tale trattamento ad ottenerne il risarcimento ai sensi dell'art. 18 anche dei danni non patrimoniali come espressamente prevede l'art. 29, comma 9.

Altre ipotesi di trattamento illecito - sanzionate anche penalmente dall'art. 35 L. cit. - possono consistere in violazioni degli artt. 11 (*Consenso*), 20 (*Requisiti per la comunicazione e diffusione dei dati*), 21 (*Divieto di comunicazione e diffusione*), 22 (*Dati sensibili*), 23 (*Dati inerenti la salute*), 24 (*Dati relativi ai provvedimenti di cui all'art. 686 c.p.p. da iscrivere nel casellario giudiziale*), 27 (*Trattamento da parte di soggetti pubblici*), 28 c. 3 (*Trasferimento di dati personali all'estero*).

**Avv. Prof. EMILIO TOSI**