a cura di Tiziano Solignani avvocato in Modena

Al via il protocollo informatico per le pubbliche amministrazioni

Il 2004 è l'anno di entrata in vigore del "protocollo informatico" per le amministrazioni. Per comprendere la portata di questa innovazione, bisogna considerare come la pubblica amministrazione sia davvero strategica per la diffusione dell'informatica nel mondo del lavoro e della vita di tutti i giorni. Oggigiorno, nei Paesi europei, allo Stato sono affidati molteplici compiti che interessano moltissimi settori della vita individuale e sociale come il lavoro, l'istruzione, lo sport solo per citare alcuni esempi di un fenomeno quotidiano e universale. Di conseguenza, le scelte tecniche delle Amministrazioni sono destinate a pesare nell'assetto informatico complessivo del Paese, perché spesso le soluzioni adottate a livello pubblico diventano poi degli standard di fatto o di riferimento. Questo è tanto vero che i movimenti per il software libero considerano già da tempo fondamentale che gli enti pubblici adottino soluzioni open source.

Una storia iniziata nel 1997

Ma che cosa si intende di preciso per protocollo informatico? In realtà, questa rivoluzione gestionale dell'operare delle amministrazioni, che dovrebbe compiersi nel prossimo periodo, era iniziata già nel 1997. Il protocollo, infatti, era stato previsto per la prima volta dall'art. 21 del DPR 513/97, il quale prevedeva che entro il 31 dicembre 1998 le pubbliche amministrazioni avrebbero dovuto provvedere alla gestione dei documenti con procedura informatica al fine di consentire il reperimento immediato, la disponibilità degli atti archiviati e l'accesso ai documenti amministrativi per via telematica tra pubbliche amministrazioni e tra queste ed i soggetti privati aventi diritto.
Sempre nel 1997, erano state varate le prime norme sul documento informatico. Il termine originariamente previsto del 31 dicembre 1998, comunque, è stato via via prorogato e l'intero sistema dovrebbe appunto entrare in vigore nel 2004.
Oggigiorno, il protocollo è confluito negli articoli da 50 a 70 del DPR 445/2000, che poi è il testo unico sulla documentazione amministrativa, da considerarsi l'attuale testo di riferimento in materia. A livello pratico, è molto importante la circolare AIPA 7 maggio 2001, n° 28, che dice come deve essere confezionato un documento da inviare alle amministrazioni che hanno adottato il nuovo sistema.

La via del digitale

Il protocollo informatico, dunque, non è altro che un sistema di memorizzazione e trasmissione di tutti i documenti delle amministrazioni in formato digitale. Il concetto, in sé banale, avrà importanti conseguenze sul modo di vivere e lavorare di noi tutti. Esso comporterà infatti, quando sarà realizzato pienamente, in primo luogo la possibilità di trasmettere alle amministrazioni documenti in formato digitale, cioè "documenti informatici", come ad esempio domande di concorso, istanze volte al rilascio di documenti, autorizzazioni, certificati, licenze, concessioni e ciò - si noti - in qualsiasi ambito di questo vasto "mare magnum" che è la Pubblica Amministrazione (per cui ad esempio patenti, concessioni urbanistiche ed edilizie, autorizzazioni, licenze per attività commerciali, rinnovi documenti e così via).
In secondo luogo, l'utente potrà accedere molto più facilmente ai documenti delle Amministrazioni, che saranno disponibili in formato digitale e accessibili per via telematica, ovviamente previa autenticazione, necessaria quando il documento non è accessibile a tutti e cioè pubblico.
Ci saranno poi anche vantaggi interni per le Amministrazioni, che tradizionalmente scontano un difetto di comunicazione tra loro e, addirittura, tra stessi uffici di un medesimo ente, dal momento che sarà sufficiente interrogare un server centrale di documenti per vedere in che stato si trova una determinata pratica presso un certo organo o ufficio.
Infine, ci sarà una molta maggiore capacità dell'Amministrazione di comunicare con gli utenti, tramite trasmissione alle caselle e-mail degli stessi di documenti rilevanti: ad esempio un'azienda potrà richiedere la trasmissione di tutti i bandi di appalto relativi ad un certo contesto territoriale ed economico, un privato tutti i concorsi per un determinato profilo professionale e così via.
Ovviamente, in tutti questi casi si avrà maggiore rapidità, efficienza, trasparenza, con riduzione del carico di lavoro dei funzionari che, liberati dallo "sportello", potranno dedicarsi più intensamente alle attività proprie dell'ufficio.

I passi

Evidentemente, il protocollo informatico potrà essere implementato solo quando saranno stati adottati compiutamente anche il documento informatico e la firma digitale, che sono i due strumenti fondamentali per realizzare il sistema di gestione documentale previsto dal protocollo. Sotto questo punto di vista, siamo certamente ad uno stato avanzato, dal momento che la firma digitale è di fatto e di diritto già stata realizzata, tanto che oggigiorno si può utilizzare tranquillamente, beneficiando di tutte le disposizioni in materia.
Per il resto, è ovvio che il passaggio al nuovo sistema richiederà uno sforzo organizzativo, gestionale ed umano enorme, vista l'importanza del cambiamento e la netta differenza tra il vecchio e il nuovo regime.

L'esempio di Torino

Comunque, per tutti coloro che intendono inviare un documento ad una amministrazione che, come ad esempio la Camera di commercio di Torino, ha già implementato il protocollo informatico, le regole da seguire sono quelle dettate dalla già vista circolare AIPA 7 maggio 2001, n° 28, cui vale comunque la pena dare un'occhiata per rendersi conto di come funzionerà il nuovo sistema.

PER APPROFONDIMENTI

www.interlex.it/pa/prot_norme.htm una raccolta di norme sul protocollo informatico
http://protocollo.gov.it/ il sito ufficiale del protocollo informatico
www.cnipa.gov.it/ il sito del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA, conosciuta precedentemente con il nome di AIPA)
www.to.camcom.it/ il sito della Camera di commercio di Torino, uno dei primi enti ad avere già implementato il protocollo informatico

a cura di Tiziano Solignani avvocato in Modena

Privacy, le novità del nuovo codice di protezione dei dati

Dal primo gennaio 2004 sarà in vigore il nuovo Codice in materia di protezione dei dati personali. Questo testo, approvato con il Decreto legislativo 30 giugno 2003, n. 196, riunifica tutta la materia precedente, abrogando tra l'altro addirittura la famosa legge 675/1996 sul trattamento dei dati personali ed il relativo regolamento di attuazione, e componendo in un'unica "legge" tutte le disposizioni in materia di privacy (per vedere il Codice integrale vi rimandiamo alla seguente pagina: www.garanteprivacy.it/garante/doc.jsp?ID=228213). Ma non si tratta solo di una raccolta, ci sono anche alcune novità che vale la pena analizzare.
Diciamo subito che gli aggiornamenti della legge riguardano in modo marcato coloro che gestiscono i dati (come ad esempio i responsabili dei sistemi informativi). Per il singolo utente consumer i diritti pregressi permangono.

Quando contattare il Garante

Il primo, molto positivo, cambiamento riguarda l'obbligo di notifica al garante che, da "generale", diventa "residuale". E quindi previsto solo in alcuni casi (si vedano gli artt. 37 e 38 del nuovo codice), fra i quali citiamo a titolo di esempio il trattamento di dati relativi allo stato di salute, alle scelte politiche o religiose, alle preferenze di acquisto, alla situazione patrimoniale, o ancora i dati sulla posizione geografica di soggetti, come nel caso delle "celle" della rete di telefonia mobile. Anche se ci sono voluti diversi anni, si è capito che inondare di carta gli uffici del Garante non porta a molti risultati e anzi implica lavoro inutile, sia per le aziende che per lo stesso ente di controllo.

Gestione semplificata

Sono poi introdotte altre modifiche volte alla semplificazione generale della gestione dei trattamenti dei dati. Il nuovo codice, infatti, si basa sul "principio di necessità", secondo cui i sistemi informativi dovranno essere in ogni caso configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. In altri termini, dovranno essere impiegate tecniche di identificazione del soggetto solo in caso di necessità in tutti i casi in cui ciò sia possibile, ad esempio associando un ID ad una determinata persona, sempre che le finalità del trattamento siano realizzabili anche in questo modo.

Le misure di sicurezza

Rimangono, ovviamente, le norme in materia di misure di sicurezza che devono essere adottate da tutti coloro che gestiscono un sistema informatico, regolate nel titolo V del nuovo codice. È al riguardo confermato che i dati personali oggetto di trattamento debbono essere custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico nonché alla natura dei dati al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
Sono le già note "misure minime di sicurezza", definite dal nuovo codice come quel complesso di misure tecniche, organizzative, logistiche e procedimentali di sicurezza che sono in grado di dare un livello minimo di protezione. Il codice si spinge oltre e identifica le singole misure da adottare definendone gli aspetti tecnici.

A) Innanzi tutto occorre predisporre l'utilizzazione di un sistema di autenticazione informatica, quindi ai computer deve potersi accedere solo ed esclusivamente previo inserimento di user name e password. La password dovrà poi essere custodita dai soggetti autorizzati in modo da garantirne la segretezza. La password, per essere a norma, deve essere composta da un minimo di 8 caratteri, salvo il caso in cui non sia possibile per il tipo di software che si sta utilizzando. Inoltre la password deve essere modificata ogni sei mesi, addirittura tre nel caso di trattamenti di dati sensibili o giudiziari, anche se è difficile capire come le Autorità potranno procedere ad accertare violazioni di questo obbligo. Le password devono inoltre essere dotate di scadenza. Le credenziali di autenticazione non utilizzate da almeno sei mesi debbono essere disattivate, derogando solo nell'ipotesi di un utilizzo meramente finalizzato alla gestione tecnica.

B) Il codice vuole poi dire la sua anche in fatto di definizione dei permessi degli utenti e dei relativi gruppi, parlando di "profili di autorizzazione". Viene specificato che i profili di autorizzazione per ciascun incaricato o per classi omogenee di incaricati, dovranno essere individuati e configurati anteriormente all'inizio del trattamento: questo al fine di limitare l'accesso ai soli dati effettivamente necessari alla realizzazione delle operazioni di trattamenti cui sono preposti gli incaricati; la verifica in relazione alle condizioni sussistenti la conservazione dei profili di autorizzazione deve avvenire almeno annualmente.
Per chi non rispetta le nuove direttive sono previste sanzioni sia amministrative che penali, anche se sono tutte da valutare le modalità di accertamento dell'infrazione.

È stato ereditato dal vecchio DPR 318/1999 l'obbligo di redazione del documento programmatico sulla sicurezza. In sostanza, entro il 31 marzo di ogni anno l'amministratore di sistema dovrebbe redigere questo documento, secondo il disciplinare tecnico allegato al codice, dove in sostanza devono essere indicate le caratteristiche del trattamento, i rischi che incombono sullo stesso, le misure intraprese e i metodi per ripristinare in caso di crash del sistema o intrusione.
Quest'obbligo suscita qualche perplessità, perché forse si poteva semplificare ulteriormente. Bisognerà vedere comunque in futuro come anche questa novità, insieme a tutto il resto del codice, verrà recepita dalle aziende e da tutti gli altri soggetti interessati ai trattamenti di dati. ■

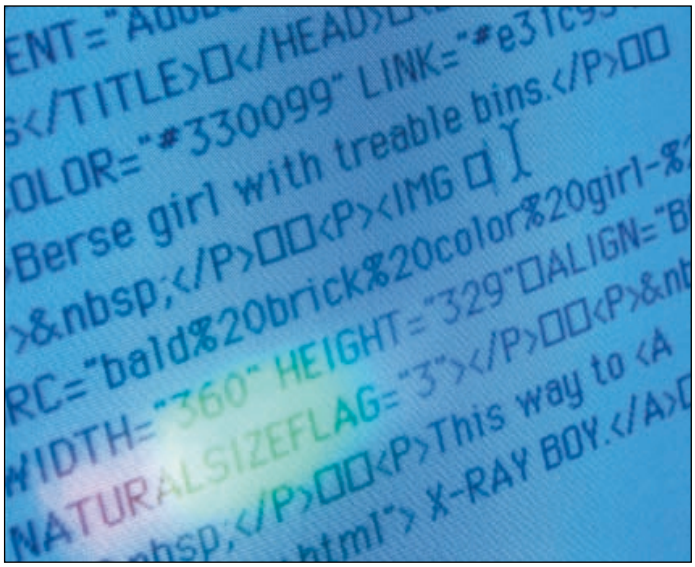
a cura di Tiziano Solignani avvocato in Modena

Lotta allo spam, i rimedi possibili

Con un provvedimento del 29 maggio 2003, diffuso in settembre, il Garante italiano della privacy ha voluto fare il punto della situazione sul fenomeno dello spam, cioè l'invio di posta pubblicitaria, indesiderata e comunque non sollecitata.
Nel frattempo, è stato anche approvato il "Codice in materia di protezione dei dati personali", la cui entrata in vigore è prevista per il 1 gennaio 2004 e che sostituirà integralmente la legge sul trattamento dei dati personali 31 dicembre 1996, n. 675, unificando tutte le disposizioni in materia e dettando, in parte, regole nuove. Ad ogni modo, lo spam, che nonostante tutto è sempre più in crescita, rischia di minare la diffusione della posta elettronica e di Internet; facilita inoltre la diffusione di virus e la possibilità che comunicazioni di contenuto osceno finiscano nelle caselle postali di bambini o adolescenti. Vediamo, quindi, come sia possibile combattere questa pratica, anche sulla scorta di quanto richiamato dall'Autorità di garanzia nel suo parere, delle iniziative adottate in questi ultimi anni e di quanto previsto dal nuovo codice, che rappresenta anche l'attuazione della direttiva 2002/58/UE in materia di dati personali e privacy.

Lo spam è un illecito penale

Bisogna dire subito che i rimedi sono diversi a seconda che si tratti di messaggi inviati dall'estero oppure di spam che ha origine in Italia. Da questo punto di vista, è importante ricordare, come dice lo stesso Garante, che lo spam è un reato, cioè un illecito penale. E non è sempre tale solo in sé stesso, come trattamento vietato di dati personali, ma a volte è il punto di partenza per tentare di commettere ulteriori reati, come ad esempio i vari tentativi di truffa, tra cui celebre è ad esempio quello del funzionario governativo nigeriano che deve far uscire dal Paese una enorme quantità di denaro, ma necessita della collaborazione di una persona esterna (che però prima deve a sua volta effettuare un versamento). La natura di reato dello spam rende in qualche modo sanzionabili anche coloro che "spammano" dall'estero.



La "spazzatura" che arriva dall'estero...

Infatti, se si riceve un messaggio di spam dagli Stati Uniti o dal Brasile, ad esempio, il Garante italiano può fare ben poco. Infatti la legislazione italiana sul trattamento dei dati personali non è applicabile in questi casi. È invece applicabile la legislazione penale. In materia vale infatti quanto previsto dall'art. 6 del Codice Penale italiano per cui "chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana".
Secondo la nostra legge, infatti, un reato "si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento" che ne consegue. Nel caso dello spam, dove il comportamento che costituisce reato è l'invio della posta elettronica, il reato potrebbe senz'altro considerarsi commesso in Italia. Inoltre quando vi è ad esempio un tentativo di truffa o l'invio di materiale pedofilo o pornografico sicuramente vi è un ulteriore reato punibile in Italia.
Rimane però comunque il problema dell'individuazione dei responsabili e dell'efficacia concreta nei loro confronti di una sentenza di condanna emessa da un giudice italiano.

..e quella che ha origine nazionale

Quando invece lo spam ha origine nazionale si applica integralmente la legislazione italiana che, tra qualche mese, sarà integrata dal nuovo codice in materia di privacy. I principi fondamentali sia della vecchia che della nuova legge rimangono sempre gli stessi e sono ricordati dal Garante. Non è possibile utilizzare indirizzi di posta elettronica presi da Internet, perché la pubblicazione di tali indirizzi da parte dei rispettivi proprietari, avvenuta o all'interno di un newsgroup o su una pagina Web o altrove, non costituisce indice di un consenso al ricevimento di messaggi pubblicitari. È quindi sempre necessario ottenere consenso "libero, specifico e informato" per potere spedire pubblicità. In molti casi, lo spam a favore di un certo soggetto è effettuato da una società "specializzata" nell'acquisizione di indirizzi di posta elettronica su Internet e nell'invio di spam agli stessi. Anche in questi casi, è responsabile il soggetto che ha commissionato l'invio, insieme a quello che lo ha materialmente effettuato, perché entrambi sono tenuti a rispettare la normativa in materia di trattamento dei dati. Si rendono in tutti i casi applicabili i diritti previsti dalla legge alla cancellazione del proprio indirizzo dalla banca dati interessata.

Cosa fare nella pratica

Ma come ci si deve muovere, concretamente, nel caso in cui si rimanga vittima di uno spam? Nel caso di un messaggio proveniente dall'estero, la cosa migliore è rivolgersi direttamente alla Procura della Repubblica competente con una denuncia penale, che dovrà essere corredata di ogni dettaglio tecnico utile per risalire al responsabile, tra cui gli headers dei messaggi in questione. Nel caso, invece, di spam proveniente dall'Italia, si possono esercitare i diritti previsti dalla legge tra cui la richiesta di cancellazione e il ricorso al Garante che, in caso di accoglimento, in molti casi ha condannato il responsabile della violazione a rimborsare le spese processuali e al risarcimento, in misura solitamente di 250 euro, oltre che a provvedere a segnalare l'intera vicenda alla Magistratura penale per l'accertamento dei relativi reati.
È evidente che però queste iniziative non vanno considerate tanto per interesse personale o per il singolo caso concreto, per il quale si fa prima a impostare un filtro della posta o ad installare un software antispam, quanto per il bene di tutti affinché lo spam sia combattuto per avere una rete più pulita e fruibile.

Per ulteriori informazioni

www.garanteprivacy.it - la home page del sito del Garante della privacy
www.garanteprivacy.it/garante/doc.jsp?ID=29840 - Parere del 29 maggio 2003 del Garante della privacy
www.privacy.it - un ottimo sito di riferimento in tema di privacy e trattamento dei dati personali
www.maxkava.com/spam/ una ottima guida per il ricorso al Garante della privacy
www.collinelli.net/antispam/ una ottima guida tecnica sul fenomeno degli spam
www.interlex.it/testi/02_58ce.htm - il testo della direttiva 2002/58/UE
www.garanteprivacy.it/garante/doc.jsp?ID=228213 - il link da cui scaricare il testo del codice in materia di protezione dei dati personali

a cura di Tiziano Solignani avvocato in Modena

Acquisti in Rete, le tutele per chi usa la carta di credito

Chi acquista on line, pagando con carta di credito, gode innanzitutto delle tutele previste dalla leggi in materia di contratti "a distanza".
Queste garanzie sono riconosciute a chi fa shopping via Internet perché in questi casi il consumatore - a differenza di quanto accade nel negozio tradizionale - non può vedere direttamente il bene, valutarlo, commisurarlo, magari provarlo e vedere se corrisponde ai suoi desideri. Quindi, in primo luogo, è riconosciuto un **diritto di recesso**, esercitabile per qualsiasi motivo, entro termini previsti dalla legge, in modo diverso a seconda dei casi.
I contratti a distanza sono comunque regolati, principalmente, dal Decreto Legislativo 22 maggio 1999, n. 185 e dal precedente Decreto Legislativo 15 gennaio 1992, n. 50. Fino a che le due leggi non verranno "fuse" in un apposito testo unico, continueranno ad applicarsi entrambe, scegliendo volta per volta la disposizione più favorevole al consumatore.
Sono, poi, previste tutele ulteriori nel caso in cui il pagamento avvenga tramite carta di credito, visti i rischi di utilizzo improprio della medesima da parte di terzi malintenzionati.
La tutela principale è oggi posta dall'art. 8 del Decreto Legislativo 22 maggio 1999, n. 185, secondo cui "l'istituto di emissione della carta di pagamento riaccredita al consumatore i pagamenti dei quali questi dimostri l'eccedenza rispetto al prezzo pattuito ovvero l'effettuazione mediante l'uso fraudolento della propria carta di pagamento da parte del fornitore o di un terzo".

Il diritto del rimborso

Quindi il consumatore ha sempre il diritto di ottenere il rimborso. Ma come si fa a dimostrare che un pagamento non era dovuto? Negli acquisti on line in realtà il problema non si pone visto che non viene sottoscritta la cosiddetta "nota di spesa" e quindi il cliente può sempre richiedere il rimborso.
La nota di spesa è il bigliettino che, negli acquisti tradizionali, il cliente titolare di carta sottoscrive di suo pugno e rilascia al fornitore.
Per la legge italiana l'esistenza di una nota di spesa, cioè di un documento firmato dal titolare della carta, è sempre e comunque necessario per ottenere il pagamento. Considerando che negli acquisti in Rete non è prevista la firma di una nota di spesa, è l'istituto bancario che deve dimostrare l'esistenza di un valido giustificativo. Se non esiste, le somme devono essere riaccreditate. C'è una sola cosa che la banca può invocare a sua discolpa. Il titolare della carta ha infatti, per contratto, un preciso dovere di custodia della stessa.
La banca potrebbe imputare al consumatore di essere stato eccessivamente imprudente nel comunicare gli estremi della propria carta a sconosciuti e sostenere pertanto che ogni conseguenza negativa di ciò debba andare, per sua colpa, a suo scapito. Ciò nella prassi non si è ancora verificato, perché gli Istituti di credito in questi casi preferiscono dar luogo ai rimborsi.

Nella pratica

Come muoversi, allora, quando si notano voci di spesa nel proprio estratto conto che non sarebbero dovute esserci? La cosa migliore è scrivere subito una lettera raccomandata diretta alla sede legale di:
a) banca;
b) società gestrice della carta;
c) se possibile ed identificabile: fornitore.
In tale comunicazione, si dovrà richiedere il rimborso della somma illegittimamente addebitata, da indicare con precisione, specificandone i motivi e cioè che non corrisponde ad alcun acquisto, che la somma era minore, che il sito che pare essere destinatario del pagamento non è mai stato frequentato e così via.
Parallelamente, bisogna recarsi dai Carabinieri della più vicina stazione e sporgere formale denuncia-querela per il reato di indebito utilizzo di carta di credito o per gli altri che saranno ravvisati nella vicenda in questione, esponendola nel modo più preciso possibile ed allegando, possibilmente, i documenti del caso, tra cui senz'altro l'estratto conto della carta di credito.
Per chi utilizza indebitamente una carta di credito, è previsto un reato apposito, definito dalla legge 5 luglio 1991, n. 197, all'art. 12, secondo cui "chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni".

Alcuni suggerimenti

A oggi, la sicurezza totale è garantita solo dai siti di commercio on line che implementano il sistema della firma digitale e, ovviamente, bisogna avere una firma digitale. In questo modo, la sicurezza della transazione è garantita dalla "chiusura" della stessa con firma digitale, con meccanismi ai quali la legislazione italiana riconosce già ora pieno valore. I siti però che offrono questa possibilità sono pochissimi e sono altrettanto pochi gli utenti Internet che dispongono di firma digitale o la usano correntemente.
Pertanto, naturalmente, il primo consiglio è quello di non usare la carta di credito per fare acquisti su siti poco conosciuti: in questi casi è meglio utilizzare altri sistemi di pagamento a distanza come il bonifico bancario, rimessa su conto postale e così via. Anche, poi, con i grandi e più rinomati siti di e-commerce c'è il rischio (remoto) che i dati inviati vengano carpiti da terzi malintenzionati: in questi casi, meglio inviare gli estremi della propria carta di credito via fax, come molti siti consigliano espressamente di fare, oppure utilizzando i form con connessione sicura (con protocollo HTTPS). Evitare infine di fornire gli estremi della carta di credito tramite posta elettronica. ■

a cura di Tiziano Solignani avvocato in Modena

Come comprare on line in sicurezza

La Polizia di Stato (www.poliziadistato.it) ha recentemente diffuso una "circolare" in cui ha messo in guardia contro le truffe telematiche. Il navigatore Internet è infatti insidiato dai malintenzionati in vario modo. Ne sono esempi le finte vendite all'asta sul Web, con merci offerte e mai inviate ai clienti o con prezzi gonfiati, l'offerta di servizi gratis su Internet che poi si rivelano a pagamento, gli schemi di investimento a piramide e multilevel business, le offerte di lavoro a casa con acquisto anticipato di materiale necessario all'esecuzione di tale lavoro e i numeri a pagamento (tipo 899) da chiamare per scoprire un ammiratore segreto o una fantomatica vincita di vacanze o di oggetti.
In alcuni casi, è più facile scoprire l'inganno, perché si tratta di stratagemmi noti da tempo, come il "lavoro a domicilio", o assai poco verosimili, come l'"ammiratore segreto".
In diverse altre ipotesi, come nel caso di una compravendita di un oggetto, almeno apparentemente normale, è invece molto più difficile. Si sono verificati, infatti, anche casi di oggetti promessi in vendita a diverse persone, pagati da molte di esse e mai consegnati ad alcuna.
Vale la pena, dunque, esaminare le tutele di chi acquista via Internet e, soprattutto, esaminare gli accorgimenti pratici per evitare di cadere in una trappola telematica per vedere infine quello che rimane da fare nelle ipotesi in cui purtroppo, nonostante tutto, l'inganno ha funzionato.

Contratti a distanza, le tutele del consumatore

I consumatori sono notoriamente tutelati da una serie di leggi dettate appositamente per i contratti a distanza, tra cui principalmente il **Decreto Legislativo 22 maggio 1999, n. 185**, entrato in vigore il 19 ottobre 1999, e il più risalente Decreto Legislativo 15 gennaio 1992, n. 50, che continua ad applicarsi quando è più favorevole al consumatore.
Tali leggi riconoscono all'acquirente il diritto di recesso entro un certo termine (solitamente 10 giorni) e prevedono l'inefficacia di molte clausole a loro sfavore. Ma bisogna dire che queste disposizioni non servono a molto in questi casi, perché sono destinate a operare prevalentemente con venditori sostanzialmente onesti e non invece nei confronti di veri e propri delinquenti che sfruttano la Rete per compiere delle truffe.
Se non altro, queste leggi prevedono una serie di informazioni che il venditore deve fornire al compratore, in tema di caratteristiche della compravendita ed esercizio del diritto di recesso, la mancanza delle quali deve mettere in guardia il navigatore. Questi, tuttavia, deve stare molto attento perché anche i truffatori sono abili nell'imitarle, un po' come fanno gli spammer quando inseriscono nelle loro mail le diciture più improbabili.

Il valore legale della posta elettronica

Occorre dunque che il navigatore cerchi di essere il più possibile accorto. Sotto questo punto di vista, un errore molto comune è quello di considerare la posta elettronica, cioè i messaggi ricevuti dal venditore, come una prova scritta idonea a garantire la sicurezza della "transazione".
Questo non è vero, se non in minima parte. Se le e-mail inviate dal presunto venditore non erano firmate digitalmente, cosa che ovviamente non si ha mai quando si compiono delle truffe, non c'è modo di dimostrarne la provenienza e la paternità. Tali messaggi non sono nemmeno dei documenti, perché non portano la firma del loro autore.
L'unico modo per risalire al computer dal quale sono state spedite è ricostruire l'intero percorso tramite l'indirizzo IP da cui sono state generate e i log dei provider, quantomeno di quello di apparente origine (salvo poi scoprire che vi è di mezzo un anonymous remailer o che è impossibile comunque risalire all'effettivo titolare dell'account di partenza).

Pagamenti in contanti da evitare

Un altro errore che a quanto pare si verifica nella pratica ma che è sicuramente da evitare è quello di pagare il prezzo degli oggetti in contanti. In caso di problemi, non sarà mai possibile dimostrare che è stato eseguito un pagamento.
La cosa migliore è pagare ovviamente in contrassegno, anche se questo non garantisce dall'invio di pacchi contenenti merce non corrispondente, o almeno tramite vaglia postale o bonifico.
Se si rimane vittima di quella che, tutto considerato, sembra proprio una truffa, la cosa più indicata è presentare una querela, lasciando perdere, almeno in un primo tempo, le cause civili.
La denuncia può essere presentata entro tre mesi dal giorno in cui il reato è stato compiuto, quindi meglio farla prima possibile. In tale documento, che può essere presentato presso la locale stazione dei Carabinieri, devono essere esposte con precisione le circostanze del fatto, allegati i documenti relativi allo stesso, anche le copie delle e-mail nonostante il poco valore, indicati gli eventuali testimoni che hanno seguito i fatti e richiesta la punizione del responsabile, per la individuazione del quale bisogna cercare di indicare tutto quello di cui si è a conoscenza. Nonostante la obbligatorietà dell'azione penale, è improbabile che denunce come queste, se rimangono isolate, ottengano grande attenzione: è più facile che vengano seguite maggiormente nel caso in cui le vittime siano state più di una, in modo che ogni procedimento sia poi riunito. ■

ALCUNI CONSIGLI

1) La prima cosa da evitare è pagare in contanti. Se viene richiesto un pagamento in contanti dal venditore, è bene accertarsi nuovamente della sua "affidabilità", perché nessun operatore commerciale serio e spesso nemmeno i privati usano questo sistema. In ogni caso non sarà possibile in caso di problemi dimostrare che si è effettuato un pagamento.
2) Non fare mai affidamento sul valore di documento dei messaggi di posta elettronica ricevuti. Se non sono firmati digitalmente, non hanno valore di prova per la legge italiana e, da soli, non servono per poter denunciare il venditore in caso di problemi.
3) Può essere utile controllare le informazioni fornite dal venditore che devono essere conformi alle leggi in materia, tra cui il Decreto Legislativo 9 aprile 2003, in vigore dal 14 maggio scorso, facendo però attenzione che potrebbero anche essere state abilmente "imitate" proprio con lo scopo di acquisire un'apparenza di serietà.
4) Eventualmente può dare qualche risultato fare una ricerca con Google nelle pagine Web o nei gruppi, cioè nell'archivio dei newsgroup, con il nome del venditore e/o le caratteristiche dell'oggetto.

a cura di Tiziano Solignani avvocato in Modena

Transazioni on line, luci e ombre della nuova direttiva

Con il decreto legislativo 9 aprile 2003, in vigore dal 14 maggio scorso, è stata data attuazione nel nostro Paese alla direttiva dell'Unione 2003/31/CE, relativa alla cosiddetta **information society** e al commercio elettronico.
Con tale provvedimento è stato varato un piano pluriennale volto ad incentivare la realizzazione di una società in grado di sfruttare consapevolmente le possibilità messe a disposizione dalle nuove tecnologie ed in cui tutti possono godere in modo appropriato dei vantaggi delle telecomunicazioni.
Lo scopo del Consiglio sarebbe non solo quello di tutelare i cittadini comunitari, consentendo loro di utilizzare nuovi strumenti di lavoro e svago, ma anche quello di migliorare il ruolo e la visibilità dell'Europa nel contesto mondiale, nella convinzione che una maggior implementazione della information society non possa che dare maggior smalto a tutti i paesi dell'Unione.
La legge stessa definisce il suo ambito di applicazione, mediante la definizione di "servizio della società dell'informazione", e pone, poi, una serie di regole per chi eroga tali servizi, tra le quali sono particolarmente interessanti quelle in materia di informazioni da inviare ai consumatori e di comunicazioni commerciali non sollecitate o spam.

Più tutela per i consumatori

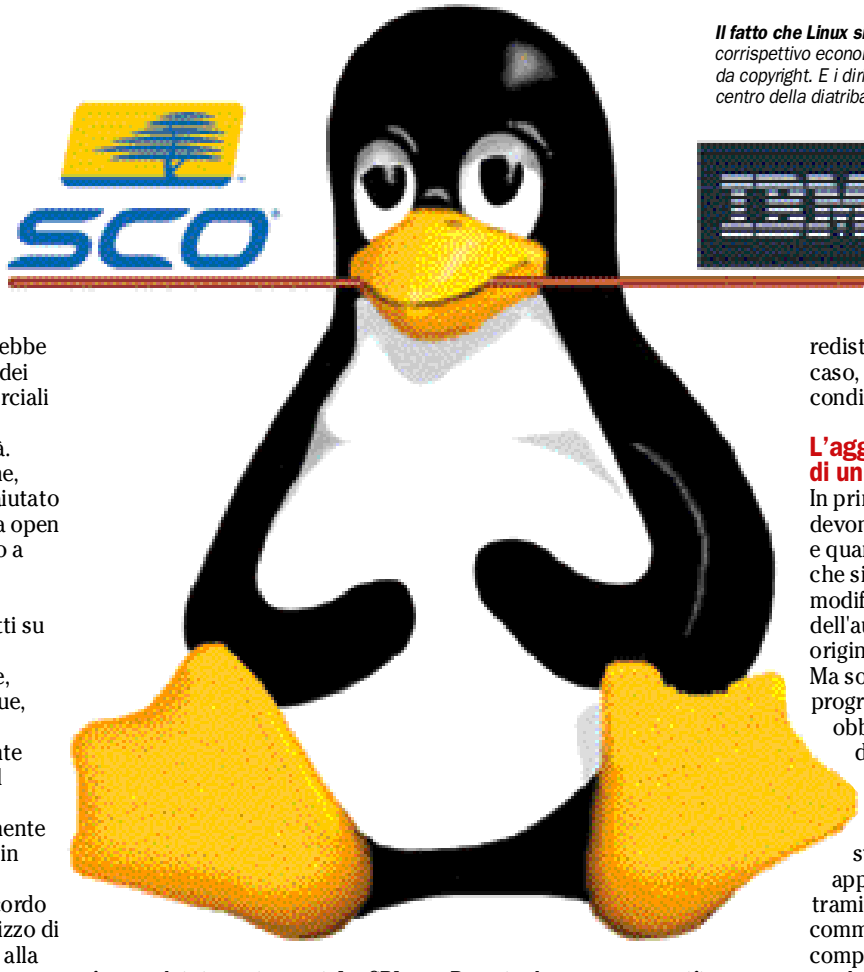
Servizio della società dell'informazione è qualsiasi servizio prestato normalmente dietro retribuzione a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione e di memorizzazione dei dati, a richiesta individuale di un destinatario di servizi. Si tratta, in primo luogo, dell'offerta di beni o servizi in rete come le vendite di hardware, software, assicurazioni, consulenze e così via. Ma sono compresi anche i servizi che non sono pagati da chi li utilizza, nella misura in cui costituiscono un'attività economica.
La legge si riferisce a quelle iniziative che non si finanziano richiedendo un corrispettivo agli utenti, ma tramite la raccolta pubblicitaria.
Esistono infatti siti che forniscono informazioni di qualità a livello professionale ed il cui accesso rimane completamente gratuito per l'utente. Non rientrano invece nella definizione di servizio della società dell'informazione tutte le comunicazioni che avvengono tra soggetti che operano al di fuori della loro attività imprenditoriale o professionale - il cosiddetto C2C, **consumer to consumer**. Una transazione tra utenti di e-bay, ad esempio, per la vendita di un computer non è soggetta alla nuova legge.
E' ovvio, poi, che le nuove regole non si applicano solo in Italia ma in tutti i paesi facenti parte della Unione Europea, quindi il consumatore potrà in qualche misura fare affidamento sulle stesse, anche se il modo in cui la direttiva è stata attuata potrà variare da paese a paese. Una cosa importante è che in materia di giudice competente in caso di problema, la nuova legge non ha cambiato nulla: come in precedenza, il consumatore italiano, ad esempio, che ha una vertenza con un sito di e-commerce tedesco può sempre rivolgersi al giudice del suo luogo di residenza.
La direttiva 2003/31, comunque, conferisce da questo punto di vista una tutela maggiore al cittadino che acquista beni o servizi da altri paesi della Comunità.

Spam e messaggi pubblicitari

Le prescrizioni imposte dalla nuova legge a chi eroga servizi per via telematica sono diverse. Tra le più interessanti sono le prescrizioni in materia di informazioni obbligatorie e di **spam**. L'articolo 8 dispone infatti che le comunicazioni commerciali che costituiscono un servizio della società dell'informazione o ne fanno parte integrante devono contenere, sin dal primo invio, ed in modo chiaro ed inequivocabile, le seguenti indicazioni:
a) che si tratta di comunicazione commerciale;
b) la persona fisica o giuridica per conto della quale è effettuata la comunicazione commerciale;
c) che si tratta di un'offerta promozionale come sconti, premi, o omaggi e le relative condizioni di accesso;
d) che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione.
Questa disposizione, per la verità, non è molto innovativa dal momento che c'era già un obbligo analogo, previsto dall'art. 3, comma 3°, del Decreto Legislativo 185/1999 in materia di contrattazione a distanza, di cui la nuova legge rappresenta una puntualizzazione ed un rafforzamento.
In tema di spam, cioè di invio di "comunicazione commerciale non sollecitata", l'art. 9 prevede che le comunicazioni commerciali debbano essere identificate come tali sin dal primo invio e contenere la specifica che il destinatario può opporsi al ricevimento in futuro di tali comunicazioni.
Di fronte a questa regola, è lecito chiedersi se non si sia fatto un passo indietro, piuttosto che avanti, nella lotta allo spam. Anche perché è stato completamente ignorato l'articolo 7 della Direttiva, secondo cui gli Stati avrebbero dovuto adottare "i provvedimenti necessari per far sì che i prestatori che inviano per posta elettronica comunicazioni commerciali non sollecitate consultino regolarmente e rispettino i registri negativi in cui possono iscriversi" coloro che non vogliono ricevere tali comunicazioni. In sostanza, la direttiva prevedeva l'istituzione di una **black list** alla quale chiunque avrebbe potuto iscriversi e verso i cui indirizzi nessuno avrebbe potuto mandare comunicazioni non sollecitate. Nella nuova legge, però, questo non è stato previsto. Anzi, l'art. 9 sembra quasi tornare indietro, passando dal sistema, sino ad ora implementato, dell'**opt-in**, dove è necessario il consenso del destinatario per inviargli posta, a quello dell'**opt-out**, dove al destinatario si lascia solo la libertà di richiedere la cessazione dell'invio. Si tratta di una novità poco felice della legge attuativa e si spera che il testo unico sulla privacy che dovrebbe essere di imminente emanazione vi ponga rimedio. ■

***La direttiva 2003/31/CE** fissa i paletti per il commercio elettronico, ma sullo spam si rischia di fare un passo indietro*

Linux, SCO e IBM combattono per il copyright



Il fatto che Linux sia utilizzabile *senza pagare un corrispettivo economico, non significa che sia esente da copyright. E i diritti di utilizzo dei brevetti sono al centro della diatriba fra SCO e IBM*

La società californiana SCO, attuale titolare del copyright sul sistema Unix ha recentemente fatto causa ad IBM chiedendo un miliardo di dollari di risarcimento perché quest'ultima a suo dire si sarebbe appropriata illegalmente della tecnologia Unix di SCO, integrandola all'interno di Linux. IBM avrebbe sfruttato a questo riguardo dei veri e propri segreti commerciali acquisiti durante la collaborazione fra le società. Secondo SCO, in conclusione, IBM avrebbe illecitamente aiutato lo sviluppo del noto sistema open source grazie al suo accesso a Unix. Ragionando in questo modo, SCO ritiene di poter legittimamente vantare diritti su ogni copia di Linux in circolazione, tant'è vero che, dopo la causa contro Big Blue, SCO ha anche inviato 1500 lettere di diffida ad altrettante aziende i cui server usano il software del pinguino. La situazione si è poi ulteriormente complicata quando è scesa in campo Microsoft, per concludere una sorta di accordo di licenza con SCO per l'utilizzo di UNIX, in sostanza aderendo alla sua tesi.

Linux, terra di nessuno?

In ogni caso, qualunque sia l'esito della vertenza SCO-IBM, le notizie che negli ultimi mesi hanno investito Linux e le modalità di licenza testimoniano quanto la questione sia ancora lungi dall'essere risolta. Linux è infatti comunemente considerato come una sorta di "terra di nessuno", un software completamente "libero" da copyright e altri vincoli.
In realtà, le cose non stanno così. Il fatto che Linux sia utilizzabile senza pagare corrispettivo non significa che Linux sia esente da copyright, come molti sono erroneamente portati a credere. Linux è oggetto di diritto d'autore, per la precisione a favore del celebre Linus Torvalds, così come lo sono tutti gli altri software rilasciati con la GPL, a favore dei rispetti autori. La GPL è contro gli scopi per cui viene utilizzato tradizionalmente il copyright, ma di fatto lo usa ed è anzi interamente costruita sul sistema del diritto d'autore, sia pure per obiettivi opposti a quelli soliti. La GPL infatti tramite le regole del copyright vuole garantire la libertà di utilizzo e scambio del software per tutti.

La licenza GPL

In primo luogo, l'utente di un software regolato dalla GPL ha il diritto di usare il programma, di farne ulteriori copie per uso personale, di redistribuirlo liberamente. L'unico vincolo che è previsto in caso di redistribuzione è che ogni copia deve essere accompagnata dall'indicazione del titolare del diritto d'autore sul programma (copyright) nonché da copia della licenza GPL.
Deve inoltre essere specificato che non ci si assume alcuna responsabilità circa il funzionamento del software in qualsiasi ambito. Le aziende che si occupano della distribuzione di software possono richiedere un corrispettivo, ad esempio per il lavoro di raccolta del software libero su di un CD ROM o in altra banca dati, quindi mettere sul mercato raccolte di software libero.
Altre aziende possono inoltre offrire consulenza a pagamento circa l'installazione e il funzionamento del software libero.
Il software libero, inoltre, può essere modificato e personalizzato dall'utente, in modo da venire incontro alle sue particolari esigenze. In molti casi, viene realizzato un nuovo software basato su di un precedente software open source "di origine". Questo nuovo lavoro può essere non solo utilizzato da chi lo ha sviluppato, ma anche ulteriormente redistribuito: in quest'ultimo caso, tuttavia, ci sono alcune condizioni da rispettare.

L'aggiornamento di un software open source

In primo luogo, i file modificati devono recare l'indicazione di chi e quando li ha cambiati, in modo che si possa capire che le modifiche non sono opera dell'autore del programma di origine.
Ma soprattutto, il nuovo programma deve obbligatoriamente essere distribuito sotto la licenza GPL. Un'azienda, in altri termini, non può prendere un software GPL, svilupparci "sopra" un altro applicativo e rivenderlo tramite la concessione di licenze commerciali. Questo è vietato e comporta violazione della GPL, per la quale il titolare del copyright sul software di origine può agire nei confronti dell'azienda richiedendo i danni. Per questi motivi, la licenza GPL è considerare una "licenza virus", perché tutto quello che viene costruito sopra software rilasciati con la GPL deve obbligatoriamente seguire lo stesso regime. Ovviamente lo scopo è quello di tutelare al massimo grado lo sviluppo e la diffusione del software libero. In fondo è anche giusto: se una azienda vuole realizzare un prodotto commerciale, può scriverlo benissimo ex novo. Se invece vuole risparmiare il lavoro di programmazione, non può prendere un software libero, personalizzarlo e rivenderlo guadagnando in sostanza sul lavoro che era stato fatto da altri disinteressatamente a favore della comunità. ■

Linux e il “copyleft”, il diritto d’autore alza la voce

La licenza GNU-GPL è quel tipo molto particolare di licenza software con cui vengono rilasciati i programmi cosiddetti "open source". Lo stesso sistema operativo Linux, ad esempio, è rilasciato con la GPL, acronimo che sta per *General Public License*, messa a punto dalla Electronic Frontier Foundation fondata da Richard Stallman.
Il testo originale della licenza, in lingua inglese, si può reperire al sito della fondazione o a quello del progetto GNU (www.gnu.org) e detta le condizioni di utilizzo del software che è stato rilasciato al pubblico sotto questa formula.
Si noti che, al contrario di quello che si potrebbe pensare in un primo momento, una parte molto consistente di programmi è assoggettata alle regole della GPL: oltre al sistema operativo Linux, si pensi ad esempio ad Apache, il server Web attualmente più diffuso.
Vale la pena quindi soffermarsi sul contenuto di tale licenza e sulle possibilità che offre sia agli utenti finali, privati o aziendali, sia agli sviluppatori.

***Anche il software GNU-GPL** è oggetto di diritto d'autore. Il programma deve essere redistribuito sempre comprensivo di sorgenti e deve indicare quali parti del codice originario sono state modificate*

L’acquisto della licenza

La prima evidente differenza che la licenza GPL presenta rispetto a quella commerciale sta nell'assenza di corrispettivo: il software può essere utilizzato da tutti nei modi consentiti dall'autore senza che si debba pagare un "prezzo" come avviene invece per i prodotti commerciali, per i quali si parla, non a caso, di "acquistare" una licenza.
Lo scopo della GPL non è infatti quello di far guadagnare l'autore del software, piuttosto quello di garantire e tutelare la libertà del software, intesa come facoltà dell'utente finale innanzitutto di usare anche lui il programma, ma anche di vederne il codice sorgente, modificarlo, costruire sullo stesso un ulteriore programma.

Il copyleft e il copyright

Per perseguire questi obiettivi, e rimarcare la contrapposizione tra licenze commerciali e GPL, si è parlato di "copyleft".
Il copyleft è un gioco di parole difficilmente traducibile in lingua italiana utilizzato per la prima volta proprio dal fondatore della Electronic Frontier Foundation, con il quale si vorrebbe manifestare una chiara presa di posizione contro il copyright, cioè il tradizionale diritto d'autore. Con il copyleft, i fautori della GPL - giocando sul significato ambiguo della parola "left" che in inglese significa sia "sinistra" sia "lasciato", in contrapposizione a "right", che significa "destra", oltre che "diritto" - intendono sottolineare come con la loro licenza i diritti vengano "lasciati" all'utente a differenza che con il diritto d'autore, dove l'utente è privato di alcune libertà giudicate fondamentali dai sostenitori del software libero.

Le ripercussioni legali

In realtà il concetto di copyleft non ha molto significato sul piano legale, cioè di quello che può fare o non può fare l'utente del software oggetto di tale concessione. Inoltre, la licenza GNU-GPL non ripudia affatto il tradizionale sistema del copyright, ma tutto all'opposto, è interamente costruita sullo stesso. Il software GNU-GPL è oggetto di diritto d'autore, non è libero o freeware, e questo è testimoniato dal suo assoggettarsi alla licenza GPL, con la quale il titolare del copyright determina cosa possono fare i licenziatari. Tutto quello che non è autorizzato dalla licenza GPL non si può fare e, se viene fatto, costituisce violazione delle disposizioni in materia di diritto d'autore. La differenza, della GNU-GPL con la tradizionale licenza commerciale è che mentre la licenza commerciale usa il sistema del diritto d'autore, inteso come complesso di norme per regolare il diritto di fare copie (copyright) di un'opera intellettuale come il software (allo scopo di garantire un reddito o profitto all'autore o editore), la GPL usa sì lo stesso strumento ma per garantire la flessibilità, la possibilità di distribuire il software e l'esistenza di una comunità all'interno della quale sia possibile scambiarselo.

Cosa si può fare con licenza GNU-GPL

Vale la pena di vedere le principali facoltà concesse dalla licenza GNU-GPL, sia per i semplici utilizzatori che per coloro che si occupano professionalmente di software, a livello di sviluppo, distribuzione o altro.
In primo luogo, è riconosciuto a qualunque utente il diritto di fare copia del software e redistribuirlo ulteriormente completo del suo codice sorgente, indispensabile per introdurre eventuali modifiche; l'unica limitazione in materia è che il programma sia sempre redistribuito nella sua forma originale e che sia accompagnato dall'indicazione del copyright esistente sullo stesso, dalla comunicazione che non si presta nessuna garanzia e non si assume nessuna responsabilità in ordine al funzionamento del software stesso e da una copia della licenza GNU-GPL.
Il distributore di software open source può anche chiedere un corrispettivo per il suo lavoro di raccolta, catalogazione, messa a disposizione e così via e può inoltre, se intende offrire consulenza e assistenza su di un certo software, parimenti chiedere un corrispettivo.
Gli sviluppatori, infine, possono modificare in tutto o in parte un programma GNU-GPL e redistribuirlo una volta modificato; questo tuttavia ad una serie di condizioni: **a)** anche il nuovo lavoro deve essere licenziato con la GPL; **b)** bisogna indicare quali parti sono state modificate e da quale autore in modo che non siano confondibili con quelle originarie; **c)** occorre mantenere le indicazioni sul copyright, sull'assenza di garanzia e simili che esistono in ogni software GPL. ■

a cura di Tiziano Solignani avvocato in Modena

È diventata legge la "tassa" su CD e masterizzatori

Il 29 aprile è entrato in vigore il Decreto Legislativo di attuazione della direttiva 2001/29 dell'Unione Europea in materia di diritto d'autore. Con tale provvedimento, sono innanzitutto introdotte alcune modifiche tecniche alla legge fondamentale in materia, che rimane per il nostro paese la oramai celebre 22 aprile 1941, n. 633. Ma viene previsto, soprattutto, quel "famigerato" compenso, a favore degli autori ed editori, che, al momento in cui era stato proposto, aveva sollevato moltissime polemiche da parte della comunità degli utenti dei computer e non solo.
Dal punto di vista tecnico, la legge sul diritto d'autore viene adattata alle ultime novità in fatto di riproduzione e registrazione, soprattutto a quelle ancora una volta apportate da Internet. Il copyright viene quindi esteso a tutte le possibili forme di diffusione delle opere intellettuali oggetto di diritto d'autore, tra cui la trasmissione mediante le Reti telematiche e cioè, come si dice comunemente, tramite realtà "on line". Le stesse denominazioni legislative vengono allargate e generalizzate, dal momento che la "rivoluzione informatica" in atto consente con cadenza quasi mensile l'affermazione di nuovi media. Il termine, ad esempio, "disco fonografico" viene generalizzato ed esteso a tutti coloro che sono produttori di fonogrammi.

Quando il compenso diventa una tassa

Per quanto riguarda, invece, il compenso esso è duplice e si traduce in una specie di "tassazione" sia degli apparecchi per la riproduzione che dei supporti per la registrazione. Le apparecchiature soggette al balzello sono solo quelle "esclusivamente destinate" alla riproduzione, quindi ad esempio una piastra di registrazione o riproduzione di nastri audio.
Nel testo originario, la dicitura era molto più ampia e comprendeva tutto l'hardware in qualche modo idoneo alla registrazione o riproduzione di opere, con la conseguenza che sarebbero stati tassati anche i lettori CD, i masterizzatori, forse anche gli hard disk.
Fortunatamente, la definizione è stata poi ristretta e confinata agli apparecchi che hanno come scopo esclusivo o principale di riprodurre audio o video.

Il balzello sui supporti registrabili

Sono poi tassati tutti i supporti per la registrazione, tra cui anche i famosi CD vergini masterizzabili. Le tariffe variano a seconda del tipo di supporto e a seconda della capacità, espressa in ore di riproduzione o in capacità in MB. È comunque il Ministro per i Beni culturali che stabilisce queste tariffe, con un proprio regolamento, in mancanza e nell'attesa del quale valgono sin da subito quelle previste dallo stesso decreto legislativo.
Gli importi devono essere pagati dal produttore del CD o da chi li importa sul territorio dello Stato: non solo, ma verso il Fisco è responsabile, in solido, in caso di mancato pagamento anche il distributore. È ovvio, poi, che questi costi verranno ricaricati sui consumatori finali.
Il compenso viene, da ultimo, destinato, secondo la legge, agli "autori e produttori, artisti, interpreti ed esecutori" e così via e dovrebbe essere una specie di corrispettivo per la riproduzione privata delle loro opere.

L'imposta colpisce tutti gli utilizzatori di CD-ROM

Ma ci sono diversi dubbi e perplessità non da poco. In primo luogo, l'imposta colpisce indistintamente tutti gli utilizzatori di CD-ROM, compresi coloro che ad esempio li usano per archiviare documenti di testo e file, come nel caso delle imprese. Si consideri che l'utilizzo tipico e tradizionale dei CD registrabili è proprio quello dell'archiviazione, non certo quello della collezione di file musicali. In secondo luogo, è evidente che queste disposizioni sono in contrasto con la protezione del diritto d'autore: chi copia un CD oggetto di copyright su un CD vergine soggetto a "compenso" poi può essere trascinato ugualmente in Tribunale a rispondere di violazione del diritto d'autore e può essere condannato per tale reato. ■

***Il Decreto Legislativo** entrato recentemente in vigore prevede, fra gli altri, un compenso di 0,23 euro per 650 MB di dati su CD-R e CD-RW*

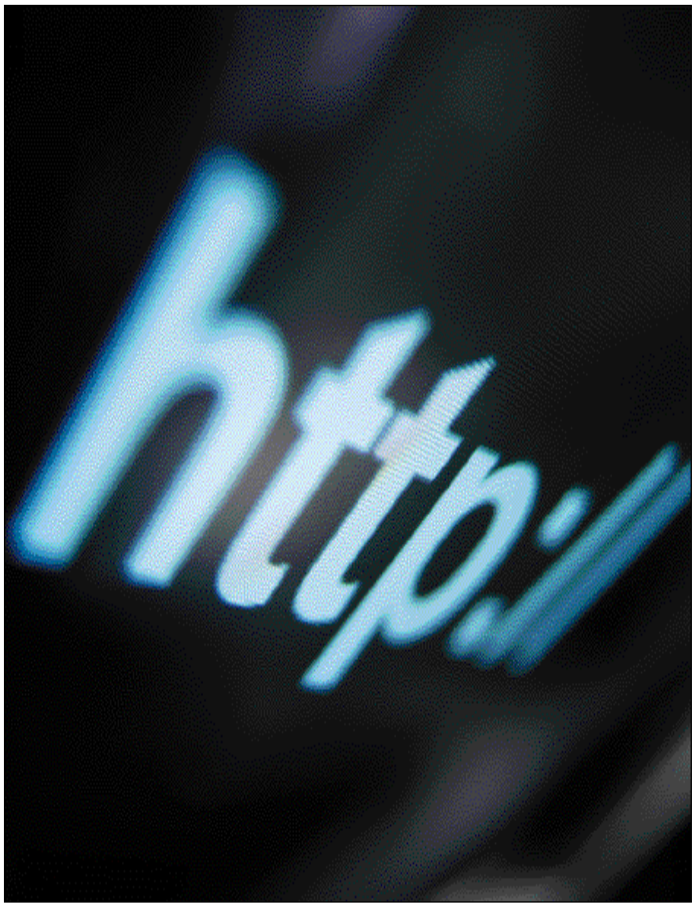
I COMPENSI PREVISTI PER I VARI SUPPORTI

I compensi previsti dal Decreto Legislativo avranno efficacia fino al 2005 ed in attesa di apposito regolamento del Ministro per i Beni culturali. Sono differenziati a seconda del tipo di supporto, e da questo punto di vista si distingue soprattutto tra supporto dedicato o multifunzione, e quindi della capacità del supporto stesso. Oltre ai supporti sono tassati gli apparecchi di riproduzione. Gli importi sono i seguenti:
1. Supporti audio analogici: ad ogni ora di registrazione corrispondono 23 centesimi
2. Supporti audio digitali (CD audio masterizzabili, minidisc e simili): per ogni ora si pagano 29 centesimi
3. CD-R e CD-RW dati: 23 centesimi ogni 650 MB
4. Flash memory e cartucce digitali: 36 centesimi per 64 MB
5. Supporti video analogici: 29 centesimi per ora di registrazione
6. Supporti video digitali "dedicati" (compresi DVD-RW e DVD-R video): per ogni ora di capacità il tributo è di 29 centesimi ed aumenta all'aumentare della durata di supporti via via più capienti
7. DVD-RW dati, DVD-R e DVD-RAM: 87 centesimi per 4,7 GB di capienza (ma aumenta proporzionalmente alla disponibilità di archiviazione)
8. Apparecchi di registrazione audio e video: il 3 per cento sul listino al rivenditore.

a cura di Tiziano Solignani avvocato in Modena

Scambio di file MP3, le responsabilità del datore di lavoro

Uno studio recentemente diffuso da una nota società di network management e analisi ha riportato come nel Regno Unito ben quattro imprese su cinque non adottino alcuna misura per impedire che i propri dipendenti usino i computer aziendali per attività di scambio di file musicali o video. Del resto, è noto che la maggior parte degli scambi di file (che non raramente superano il GB di dimensione come nel caso dei film compressi in formato DivX) avvenga tramite computer aziendali che sfruttano collegamenti professionali a banda larga e non certo tramite i collegamenti "casalinghi" che funzionano ancora in larga maggioranza via modem a 56k.
Vale la pena, comunque, di chiedersi quale sia la responsabilità del titolare dell'azienda o del suo amministratore di sistema nel caso in cui vengano trovati file MP3, AVI o simili contenenti opere coperte da diritto d'autore.
Sulla questione, la FIMI (http://www.fimi.it), cioè la Federazione dell'Industria Musicale Italiana, associazione maggiormente rappresentativa dei discografici nel nostro Paese, ha deciso di inviare alle aziende una brochure informativa, in cui si avvertono i datori di lavoro circa i "rischi connessi all'utilizzo della rete informatica aziendale per scaricare e distribuire file musicali".



Quando si commette reato

Cosa c'è di vero? In primo luogo, bisogna premettere che sicuramente fare una copia di canzoni o film o supporti analoghi oggetto di copyright è sicuramente un reato. Per la precisione, le disposizioni fondamentali in materia sono l'art. 171 e 171 ter della legge sul diritto d'autore attualmente in vigore. L'art. 171 punisce chi effettua una duplicazione abusiva di opera coperta da diritto d'autore "a qualsiasi scopo ed in qualsiasi forma" e quindi anche chi lo fa per il classico uso personale, come nel caso di colui che scarica un MP3 per ascoltarselo.
L'art. 171 ter, la norma che prevede le sanzioni più pesanti, riguarda invece chi effettua queste operazioni a scopo di lucro e comunque non ad uso personale.
Nel caso del file sharing aziendale, la disposizione applicabile sarebbe probabilmente l'art. 171, che prevede come pena una multa da 100.000 vecchie lire a 4.000.000, visto che la redistribuzione e la condivisione di file MP3 non avviene per scopo di lucro ma solo per uso personale.
Sicuramente, dunque, copiare file protetti da copyright è un reato, che comporta l'applicazione di una pena e per il quale si può essere chiamati al risarcimento del danno.

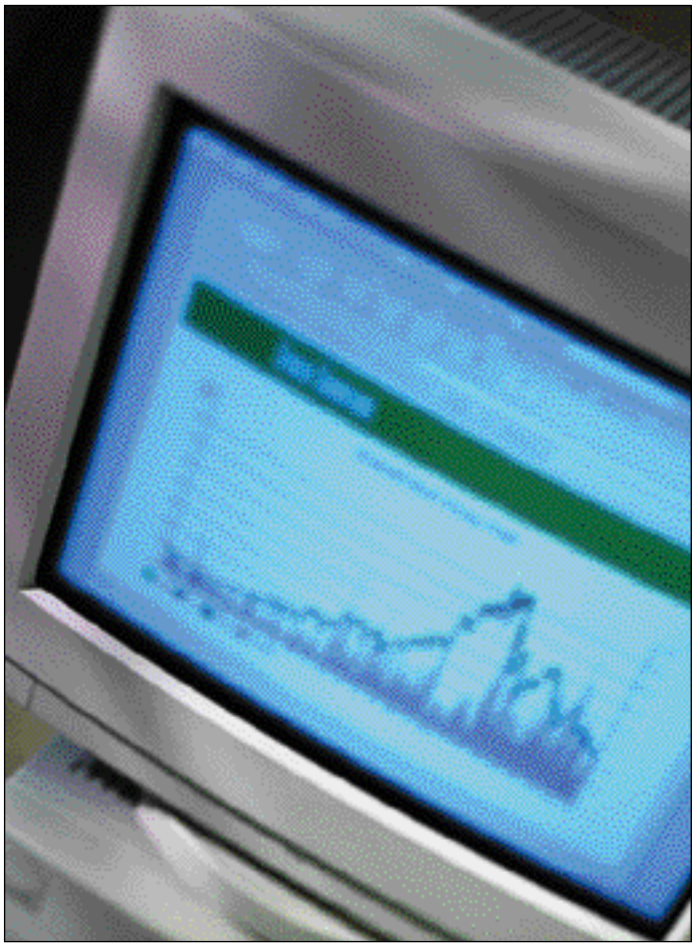
Chi è responsabile?

Ma chi può essere ritenuto responsabile se nel computer di una certa azienda si trovano illecitamente opere protette?
Il singolo impiegato che aveva in dotazione quel computer, l'amministratore di sistema oppure, ancora, il titolare dell'azienda o l'amministratore delegato che magari quel computer non lo ha mai neanche visto? Si tratta di un problema non da poco, sicuramente di soluzione molto più difficile di quello che vorrebbero far credere le associazioni discografiche. Sul punto, la legge italiana non dice nulla, lasciando che sia il giudice del caso concreto a decidere volta per volta chi può essere considerato responsabile. In linea generale, l'approccio non è sbagliato se si considerano le innumerevoli casistiche: pensiamo alla piccola azienda con tre computer e due persone che ci lavorano, tra cui il titolare; oppure la multinazionale con vari amministratori di sistema, migliaia di dipendenti, un consiglio di amministrazione, un ufficio dei sindaci.
Sarà dunque il giudice a valutare chi può essere ritenuto responsabile, valutando caso per caso. Da questo punto di vista, ovviamente, sarà molto rilevante vedere ad esempio dove, e magari su quanti computer, si trovavano i file.
Bisognerà valutare le modalità di accesso al PC che, in base anche alla normativa vigente in materia di misure di sicurezza, dovrebbero sempre prevede l'autenticazione in base a username e password. In questo modo è sempre possibile risalire all'identità degli utenti che avevano accesso ad un determinato calcolatore.
Per quanto riguarda invece le ripartizioni di responsabilità interne all'azienda, bisogna andare ad analizzare l'organizzazione del lavoro: ad esempio, nel caso sia prevista in organico la figura dell'amministratore di sistema, è difficile poter sostenere la responsabilità del datore di lavoro, mentre in caso contrario la posizione del datore diventa giocoforza più delicata.
Ad ogni modo, può essere prudente implementare misure di controllo del traffico Internet in modo da poter dimostrare quantomeno la buona fede in caso di controlli.

a cura di Tiziano Solignani avvocato in Modena

Tappe finali per l'IVA sul commercio elettronico

La Camera, nella seduta del 17 ottobre scorso, ha approvato il disegno di legge comunitaria 2002, che si trova attualmente al Senato in attesa del via libera definitivo. Il disegno di legge comunitaria recepisce una serie di direttive in materia di tutela dei consumatori e altre, tra cui anche il trattamento IVA applicabile ai servizi prestati tramite mezzi elettronici di cui alla direttiva dell'Unione Europea 2002/38/CE.
Ma quand'è che le nuove disposizioni in materia di commercio elettronico entreranno in vigore?
La direttiva dovrebbe entrare in vigore, secondo le previsioni di Bruxelles, nel luglio 2003. Bisogna però ricordare che la legge comunitaria è il principale strumento per la trasposizione delle direttive europee nell'ordinamento italiano. Introdotta nel nostro Paese nel 1989 con la Legge 9 marzo 1989, n.86, la famosa legge "La Pergola" dal nome del suo originario proponente, regola le modalità e i tempi per la trasposizione delle direttive comunitarie, determinando con quali provvedimenti (decreti legislativi, decreti ministeriali o regolamenti) deve essere attuata ciascuna direttiva, al di fuori delle ipotesi di recepimento diretto. Solitamente, la legge comunitaria contiene una serie di deleghe al Governo, il quale poi ulteriormente dovrà fare i singoli provvedimenti. La legge comunitaria, in ogni caso, non aggiunge molto a quanto già previsto dalla direttiva dell'Unione, limitandosi a stabilire, all'art. 1, che il "Governo è delegato ad adottare, entro il termine di un anno dalla data di entrata in vigore della presente legge, i decreti legislativi recanti le norme occorrenti per dare attuazione alle direttive comprese negli elenchi di cui agli allegati A e B" dove, ovviamente, nell'allegato A è riportata la direttiva IVA in



questione. Per capire quali saranno, dunque, le principali novità si può dare un'occhiata a quanto stabilito dalla direttiva stessa. Intanto bisogna dire che le nuove regole non sono state previste tanto a tutela del consumatore quanto del Fisco che, nei vari Stati, guarda da sempre al commercio elettronico come un preoccupante spiraglio per evasioni ed elusioni.
Esse comunque dovrebbero servire anche a garantire condizioni di parità per tutti gli imprenditori che intendono offrire beni o servizi a consumatori che risiedono nel territorio dell'Unione Europea.

Le transazioni soggette alla direttiva europea

La direttiva, in ogni caso, riguarderà sia le transazioni tra gli operatori commerciali (le cosiddette business to business, B2B) sia quelle con i consumatori (cosiddette business to consumer, B2C).
Le operazioni interessate saranno le seguenti:
1) progettazione, realizzazione e manutenzione di siti Web:
2) contratti di Web hosting;
3) fornitura di programmi e loro aggiornamento;
4) cessione di immagini, di musica, di film e di giochi;
5) programmi politici, culturali, sportivi, scientifici e di divertimento;
6) formazione a distanza;
7) accesso a banche dati.
Sono esclusi, invece, i servizi relativi a radio e televisione.
La "rivoluzione" della direttiva è, comunque, sostanzialmente che la prestazione viene tassata presso il committente, cioè presso l'acquirente, sia egli consumatore finale o altro imprenditore.
Quindi si applica il regime IVA previsto nel Paese in cui risiede il consumatore finale, con la precisazione che se questi risiede in uno Stato non facente parte dell'Unione l'operazione non è imponibile e non si applica quindi l'IVA.
Questo meccanismo garantisce alle imprese condizioni paritarie nel momento in cui vendono all'interno dell'Unione e condizioni addirittura di vantaggio nel momento in cui operano all'esterno.

A discapito del consumatore

Il tutto però anche a discapito del consumatore. Infatti, ad esempio, il consumatore italiano che oggi può rivolgersi alle imprese di quegli Stati in cui non è prevista l'IVA oppure è prevista un'aliquota ridotta per lo stesso bene, non potrà più farlo quando verrà attuata la nuova direttiva, perché a qualsiasi operazione che si terrà in Italia sarà applicato il regime italiano, indipendentemente dalla nazionalità del produttore. Il produttore, poi, quando andrà a vendere ad un consumatore, ad esempio, statunitense non sarà soggetto ad IVA con la conseguenza che il bene costerà meno e sarà più allettante per il consumatore residente in un Paese che non è membro dell'Unione.
Si tratta di innovazioni da seguire, dunque, con attenzione perché destinate ad incidere notevolmente sullo sviluppo e sull'incremento dell'e-commerce.
La direttiva dovrebbe inoltre avere una efficacia nel tempo limitata, di tre anni, ma non è difficile che da transitoria, quale è adesso, diventi di fatto definitiva. ■

a cura di Tiziano Solignani avvocato in Modena

Criminalità via Web, la risposta dell'Unione Europea

Per prevenire e combattere i reati, non solo quelli relativi al Web ma anche quelli più tradizionali dove Internet viene usata dagli autori dell'illecito solo per comunicare, l'Unione Europea ha elaborato, la scorsa estate, una proposta di direttiva contenente l'obbligo per i gestori delle telecomunicazioni, ed in particolare per gli Internet provider, di conservare tutti i dati relativi al traffico telefonico. La proposta si trova ancora in fase di approfondimento e vaglio da parte del Consiglio della Unione Europea, ma vale la pena soffermarsi sugli aspetti principali della stessa per gli effetti che comporterà una volta approvata.
In ogni caso, va sottolineato che si tratta sempre e comunque di una direttiva, quindi non di una legge direttamente applicabile all'interno degli Stati membri e tanto meno di un documento "invocabile" dai singoli cittadini, bensì di un atto che vincola solo gli Stati dell'Unione a emanare delle leggi di attuazione, che sono quelle di riferimento per i cittadini dei singoli Paesi. Bisognerà pertanto vedere, quando la direttiva verrà approvata e quale sarà il contenuto della legge italiana attuativa in materia.

Gli obblighi dell'Internet provider

Ad ogni modo, se la direttiva fosse introdotta, nel testo attuale, comporterebbe innanzitutto l'obbligo per tutti gli Internet provider di conservare per almeno due anni tutti i dati relativi al traffico (di qualunque genere: Web, e-mail, FTP e altro) non solo gestito ma anche in "transito".
È previsto che questa conservazione di dati sia effettuata nel rispetto delle disposizioni in materia di privacy poste dalla Convenzione Europea dei diritti umani del 1950, dalla convenzione del Consiglio europeo del 1981 sulla protezione dei diritti individuali rispetto al trattamento informatizzato dei dati personali e, soprattutto, della direttiva dell'Unione Europea del 1995, che è poi quella che ha condotto all'approvazione, nel nostro Paese, della "famosa" legge n. 675 del 1996 sulla tutela dei dati (il cui testo può essere consultato al sito www.privacy.it). Ovviamente, trattandosi appunto di una direttiva spetterà ai singoli Stati individuare le modalità concrete e tecniche con cui conciliare il rispetto delle fondamentali esigenze di tutela degli individui con la conservazione, sostanzialmente, di tutto il traffico internet su qualsiasi Internet provider: si tratterà, probabilmente, soprattutto di imporre ai provider, oltre che di conservare i dati, anche di adottare misure di sicurezza tali da impedire che i dati così mantenuti possano essere carpiti da terzi malintenzionati, come i famosi hacker o cracker.

Prevenzione del crimine

Il classico rovescio della medaglia, infatti, della creazione di database per scopi "benefici" è sempre ovviamente la possibilità che questi dati possano essere presi ed utilizzati da malintenzionati che riescono ad entrare nel database stesso. Un aspetto importante della direttiva, comunque, è che la conservazione dei dati da parte dei provider avverrà solo ed esclusivamente per scopi di "prevenzione del crimine". Quindi si deve presumere che l'utilizzo dei dati potrà avvenire solo da parte dei giudici o della polizia giudiziaria (carabinieri, polizia, guardia di finanza e simili) che indagano sull'avvenuta commissione di reati e non anche in altri casi, cioè da parte di privati oppure di altri organi dello Stato che non hanno competenze in materia penale.

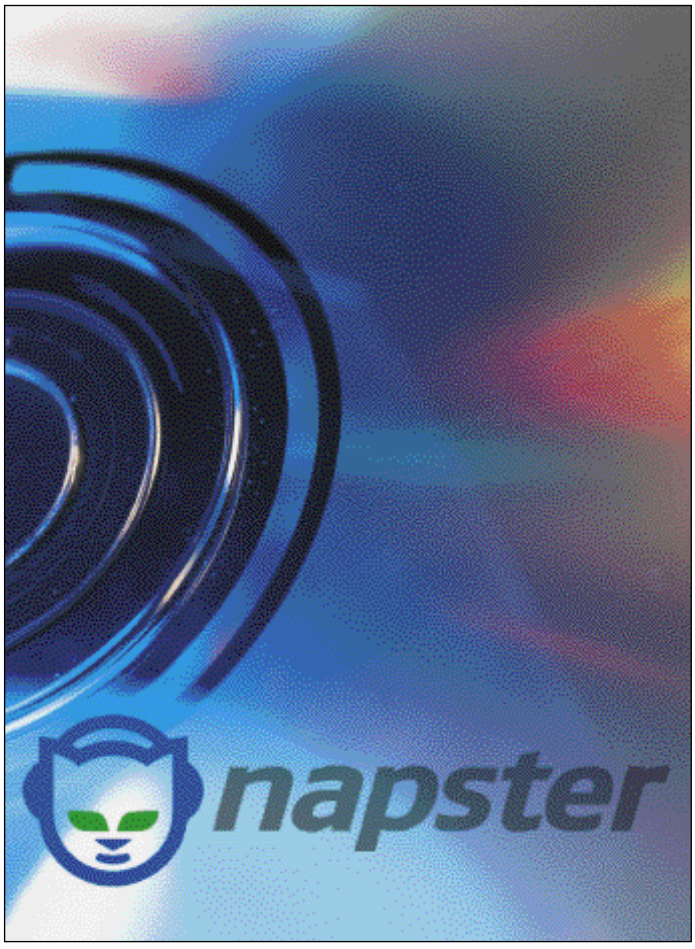
Un'Europa "unita"

La direttiva, in materia, prevede inoltre, giustamente, che il giudice o comunque l'investigatore di uno stato membro potrà richiedere i dati ai provider di tutti gli altri stati membri, i quali saranno obbligati a fornirglieli. Si tratta, evidentemente, di una previsione necessaria se si vuole che la direttiva serva a qualcosa, dal momento che è proprio sfruttando la globalizzazione della Rete che le organizzazioni criminali riescono ad operare indisturbate e a non farsi tracciare. In quest'aspetto sta anche il limite della direttiva, che purtroppo coprirà solo il territorio dell'Unione, senza possibilità per i giudici di acquisire dati da provider che si trovano in paesi extraeuropei, salva la improbabile collaborazione spontanea dei soggetti coinvolti o delle relative Autorità. ■

a cura di Tiziano Solignani avvocato in Modena

I nipotini di Napster alle prese con la legge sul diritto d'autore

L'esperienza di Napster e l'andamento della sua vicenda giudiziaria, oggigiorno sostanzialmente definita, hanno messo in allarme tutto il mondo del peer-to-peer networking.
Si sta cercando di fare tesoro di quel primo, grande esperimento per cercare di capire come riuscire a portare avanti nuove iniziative in un campo, quello della condivisione dei file, che rischia di essere costantemente al limite della legalità.
Fred von Lohmann è un legale esperto in copyright nell'era digitale che collabora stabilmente per la Electronic Frontier Foundation, la nota organizzazione no profit che, sin dagli albori di Internet, segue le attività e gli sviluppi della grande Rete. Sul sito della fondazione, e precisamente all'indirizzo www.eff.org/IP/P2P/Napster/20010227_p2p_copyright_white_paper.html, si può trovare un articolo dell'avvocato von Lohmann che fa il punto della situazione, con considerazioni che, pur essendo basate sul diritto statunitense, hanno validità anche con riguardo al diritto italiano. Le regole in materia di copyright, infatti, rispondono quasi ovunque a criteri ispiratori simili e questo è sicuramente un bene in un mondo, quello di Internet, che è sicuramente globalizzato e dove pertanto è impossibile ragionare con riferimento esclusivo alla legge di un singolo Stato.



Il concetto di copyright e il peer-to-peer

Non c'è dubbio che il P2P possa prestare il fianco alle infrazioni di direttive sul diritto d'autore. Pertanto, sia per coloro che sviluppano applicazioni P2P, sia per quanti sono intenzionati ad investire sulle stesse, sia, infine, per gli utenti finali, può essere utile cercare di ricavare alcune linee guida per vedere se e come è possibile occuparsi di peer-to-peer in modo legittimo e senza comunque andare incontro a problemi legali.
Sotto questo punto di vista, bisogna far capo al concetto di diritto d'autore, che è analogo sia nell'ordinamento USA che in quello italiano ed europeo. Sono oggetto di copyright, o diritto d'autore, tutte le opere intellettuali o creazioni dell'ingegno o espressioni artistiche che possiedono caratteristiche di originalità.
Il "diritto", quindi, nasce per effetto della creazione dell'opera. Una musica, ad esempio, viene ad essere oggetto di tutela nel momento stesso in cui viene composta e/o eseguita.
Analogamente un software, un testo e così via.
Il diritto di autore è il diritto di fare copie dell'opera e spetta solo al creatore della stessa ovvero a colui al quale il diritto è stato successivamente trasferito, come nel caso della canzone che è di proprietà della casa discografica o etichetta o del libro che diviene di proprietà intellettuale della casa editrice.

Cosa è lecito fare

Per questi motivi, è sicuramente possibile utilizzare le applicazioni P2P da parte di un singolo utente finale per condividere i video delle proprie vacanze o alcune proprie fotografie che si vogliono sottoporre, ad esempio, all'attenzione di una comunità di fotografi on line per riceverne giudizi o critiche; non è invece possibile mettere in condivisione delle canzoni che si sono registrate in formato MP3 su disco fisso da un CD.
In realtà, non si è proprietari delle canzoni registrate sul CD che si è acquistato, ma solo licenziatari, anche se nel linguaggio di tutti i giorni si dice comunemente di aver "comperato" un CD.
Quello che si ha diritto di fare, infatti, è solamente di ascoltare le canzoni sul CD per uso personale, magari di fare una copia ad uso esclusivo di backup, cioè da utilizzare solo se si rovina accidentalmente il supporto principale, ma le canzoni rimangono di proprietà della casa discografica e non possono ulteriormente essere copiate né tanto meno messe a disposizione di altre che possono fare altre copie né, in generale, essere usate per scopi e in ambiti diversi da quelli previsti dall'accordo di licenza, come ad esempio suonate in pubblico.

Le responsabilità dei gestori

Da questo punto di vista, la responsabilità dei gestori di iniziative come Napster non sta nel violare direttamente il copyright ma nel fornire uno strumento che, di fatto, consente a una comunità di utenti di realizzare copie di opere coperte da diritto d'autore.
Nel caso di Napster, i giudici hanno ritenuto lo stesso responsabile delle violazioni perché, almeno in un primo tempo, si poteva scambiare qualsiasi file e il materiale non era filtrato in alcun modo.
Inoltre, i gestori del noto sistema di scambio non potevano nemmeno sostenere di non sapere che attraverso lo stesso si scambiavano file oggetto di copyright, perché addirittura sono state prodotte in giudizio alcune schermate illustrative, in sostanza delle demo, realizzate dai gestori stessi in cui tra i file che venivano mostrati come oggetto di scambio c'erano canzoni coperte da copyright.
Chi realizza una iniziativa di peer-to-peer networking deve, dunque stare attento a questi profili. In altri termini deve inserire filtri e utilizzare le tecnologie che impediscono lo scambio di materiale proibiti.
Gli utenti finali, invece, dovrebbero utilizzare i siti e i software di scambio che sono "sicuri" e che non rischiano di poterli coinvolgere in iniziative giudiziarie per violazioni del diritto di copyright. ■

a cura di Tiziano Solignani avvocato in Modena

Internet, cellulari & privacy, l'Unione europea si muove

L'Unione Europea ha recentemente varato una nuova direttiva nel campo della tutela della privacy degli utenti di comunicazioni elettroniche (provvedimento n.2002/58/CE), destinata a introdurre diverse novità in materia non solo di posta elettronica ma anche di telefonia cellulare e fissa.
È importante comprendere che con questo intervento non si è di fronte ad una vera e propria legge (già in vigore e che quindi può essere invocata da ogni cittadino europeo) ma di un atto, rivolto agli Stati membri, che indica solamente degli scopi da raggiungere.
In particolare, i vari Stati dell'Unione, tra cui l'Italia, dovranno emanare delle apposite leggi attuative entro il prossimo 31 ottobre 2003.
Questo aspetto è molto importante, perché in queste materie è naturalmente fondamentale vedere quali saranno i meccanismi tecnici in concreto previsti per dare attuazione alla normativa. In altri termini, sarà necessario che la "nostra" Repubblica italiana faccia un buon lavoro in sede di attuazione della direttiva, se non si vuole che gli obiettivi indicati dalla stessa rimangano non realizzati o comunque aggirabili dai malintenzionati. La legge attuativa, quando verrà completata, andrà a sostituire nel nostro Paese il Decreto Legislativo 171 del 1998 attualmente in vigore, e tale rimarrà sino alla nuova legge in questione, la fonte regolatrice della materia. È possibile ora passare in rassegna le principali novità della direttiva n. 58, restando inteso che comunque, sino alla sua attuazione con apposita legge, continuerà frattanto ad applicarsi il Decreto Legislativo n. 171.

Lo spam

In primo luogo, la direttiva si è occupata del fenomeno dello spam, la posta indesiderata dalla quale molti utenti di Internet sono colpiti. È previsto il divieto di inviare e-mail omettendo o camuffando il nome del mittente, nome che dovrà poi essere usato dal destinatario per inviare l'eventuale e-mail di cancellazione del servizio. La maggior parte dei messaggi di posta indesiderata in circolazione, infatti, proviene da indirizzi diversi da quelli che appaiono nell'*header* (intestazioni) del messaggio, tant'è vero che se si prova a rispondere il mail di risposta "torna indietro" con un messaggio di errore (*bounced message*). Spesso le e-mail di spam vengono mandate tramite un account costruito appositamente presso uno dei grandi provider di fornitura di accesso e di servizi di posta elettronica, account che viene regolarmente "abbandonato" dopo essere stato usato per farvi transitare i messaggi illeciti. Questa disposizione della direttiva, più che rivolgersi ai malintenzionati, è pensata per i provider, che dovranno in futuro essere più restrittivi nel concedere l'apertura di account di posta elettronica. Non è escluso che l'invio di un messaggio possa avvenire solo previa identificazione del corretto funzionamento dell'account che ne appare come mittente. Quali saranno i meccanismi tecnici adottati, si vedrà appunto in sede di attuazione della direttiva.

Cookie e spyware

La nuova direttiva regolamenta poi anche l'uso di cookie, spyware e Web bug che possano condurre a violazioni della privacy. Sono vietati infatti, a norma dell'art. 5, "l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza consenso di questi ultimi". I cookie non sono stati vietati in senso assoluto, anche perché permettono di rendere più veloce l'accesso ad alcuni servizi Internet, ma richiederanno una previa informazioni da fornire all'utente da parte del webmaster del sito in cui sono installati.
Anche lo spyware, il software distribuito in forma gratuita ma che in realtà si finanzia tramite raccolta di dati personali relativi al computer su cui è installato e successiva rivendita a terzi, in generale sarà vietato. Tuttavia c'è una importante eccezione: l'uso di questi software può avvenire "per scopi legittimi", ovvero possono essere usati dalla Magistratura nel corso delle indagini relative ad un procedimento penale.

La privacy sui telefoni cellulari

Una nuova tutela è prevista anche per i dati relativi ai telefoni cellulari che consentono di individuare il terminale, cioè di sapere dove si trova fisicamente l'utente in un certo momento: la direttiva prevede che l'individuazione locale geografica sia limitata al minimo indispensabile per consentire l'erogazione del servizio e che comunque la stessa possa essere sospesa, gratuitamente e in modo agevole, dall'utente dello stesso. Ci sono poi ulteriori disposizioni volte a garantire la privacy degli utilizzatori di telefoni mobili o fissi: l'iscrizione negli elenchi telefonici pubblici sarà possibile solo con il consenso dell'abbonato e secondo le modalità da lui scelte. Sarà possibile scegliere se inviare il proprio numero al chiamato, se rifiutare le chiamate prive di indicazione del chiamante e, più in generale, è previsto che i dati sul traffico dell'utente debbano essere cancellati o resi anonimi al termine della comunicazione (salva anche in questo caso la possibilità di conservazione per un certo periodo di tempo per finalità di accertamento e prevenzione di reati o motivi di sicurezza nazionale). ■

a cura di Tiziano Solignani avvocato in Modena

Il valore legale di un messaggio e-mail

La posta elettronica, e in genere le comunicazioni tramite computer, per la loro comodità si vanno diffondendo sempre di più, sia tra i privati che presso le aziende. Usando questi strumenti, però, sono numerose e spesso univoche le tracce che si lasciano in giro, relativamente alla propria attività, tanto che Internet, se in un primo tempo era stata ritenuta una possibile causa di illeciti, adesso viene sempre più pensata ed utilizzata come uno strumento di prevenzione.
Qual è, dunque, il valore legale di un messaggio e-mail da noi inviato e che riposa, magari da mesi o anni, nella cartella "posta inviata" del nostro client di posta elettronica? Negli USA le aziende e i loro consulenti legali se lo stanno chiedendo con sempre maggiore attenzione, visto che alcuni giudici hanno mostrato di basare le proprie decisioni su alcune e-mail rinvenute all'interno di computer aziendali che erano stati sequestrati, come ad esempio è accaduto in uno dei diversi procedimenti a carico di Microsoft per posizione dominante. Nel caso in questione è stata trovata una circolare aziendale inviata ad un gruppo di dipendenti secondo cui "per aumentare la penetrazione di Internet Explorer 4 sul mercato dei browser sarà importante utilizzare la 'leva' del sistema operativo per indurre la gente a usare Explorer e abbandonare Netscape Navigator".
Vale senz'altro la pena di chiedersi se questo possa accadere anche in Italia.

Negli Stati Uniti, i messaggi di posta elettronica assumono una valenza legale. E in Italia...

L'istituto della discovery

Bisogna dire, innanzitutto, che tra il sistema italiano e quello anglosassone ci sono notevoli differenze sulle modalità di acquisizione delle prove. Nel nostro Paese, non è previsto l'istituto della *discovery*, intesa come richiesta fatta da una parte all'altra di produrre dei documenti in giudizio. Secondo la discovery, le parti devono produrre in modo veritiero quello che viene domandato sotto pena di gravi sanzioni. In Italia esiste solo l'*ordine di esibizione*, previsto dall'art. 210 del codice di procedura civile, che il Giudice, se una parte ne fa richiesta, può emettere nei confronti dell'altra, obbligandola a produrre in giudizio un determinato documento. L'ordine di esibizione è molto più limitato della discovery e comunque se ne fa un uso piuttosto raro.

La tutela della corrispondenza

Nel nostro Paese poi la corrispondenza (ivi compresa quella elettronica) è tutelata a livello costituzionale dall'art. 15, secondo cui la libertà e la segretezza delle comunicazioni sono "inviolabili" e qualsiasi limitazione in materia può essere posta solo nei casi previsti dalla legge con provvedimento motivato dall'Autorità giudiziaria. Infine bisogna distinguere tra procedimento civile e penale. Il primo è quello intentato da un soggetto contro un altro per motivi definibili come "privati" e cioè ad esempio il pagamento di una certa somma di denaro, una locazione, un contratto commerciale, un contratto di lavoro o di collaborazione. Il procedimento penale, invece, è quello intentato, per così dire, dallo Stato nei confronti di uno o più individui che si ritiene possano avere commesso un reato, cioè un illecito di particolare gravità. Nel processo civile le regole in materia di valore di prova dei documenti sono più rigorose: perché un documento diventi piena prova in un procedimento civile occorrono dei requisiti e delle circostanze molto precise, che spesso non si hanno nelle comunicazioni via posta elettronica. Questi ultimi non sono veri e propri documenti elettronici a livello legale perché quasi mai, siglate con la firma digitale idonea ad attribuirne la paternità e a certificarne la genuinità. Nel processo penale, che si ritiene di interesse pubblico, le regole in materia di prova documentale sono molto più elastiche.

Quando le e-mail entrano nel processo

Nel procedimento penale, insomma, le e-mail rinvenute nei computer dell'azienda di cui è titolare l'investigato o dentro alla quale sarebbero stati commessi reati possono benissimo intanto entrare nel processo. Pensiamo ad esempio ad un procedimento per illecito utilizzo di software coperto da diritto d'autore in cui è stato sequestrato, come avviene sempre e regolarmente in questi casi, il computer del presunto responsabile: se il consulente tecnico nominato dalla Procura è capace ed esperto può trovare nella posta in uscita del client di e-mail o di usenet magari un messaggio di richiesta del "crack" o di copia della licenza, di fronte al quale sarà difficile per il malcapitato sostenere la sua "innocenza".
Una volta entrate nel processo, queste prove possono essere seriamente valutate dal giudice, dal momento che la definizione di documento nel procedimento penale, fornita dagli artt. 234 ss. del codice di procedura penale, è molto più ampia di quella civile e prevede l'acquisizione "di scritti o altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia la fonografia o qualsiasi altro mezzo".

La gestione dei documenti

In conclusione, è opportuno che le aziende, ma anche i privati, definiscano una certa politica di gestione delle comunicazioni e dei documenti, basata sulla "distruzione" periodica dei documenti (cosiddetto *purging*, previsto dai più diffusi client di posta e di newsgroup), anche perché certe comunicazioni, di tipo interno e confidenziale, possono essere letteralmente travisate ed assumere tutto un altro significato in ambito giudiziario. ■

a cura di Tiziano Solignani avvocato in Modena

Nuova legge sulla garanzia, domande e risposte

La "rivoluzione" nel settore delle garanzie sui beni di consumo introdotta con il D.Lgs. 2 febbraio 2002, n. 24 è ricca di conseguenze sul piano pratico che richiedono ancora diverso tempo per essere assimilate sia dai fornitori che dai consumatori. Per questo motivo, e spinti anche dalle richieste in merito dei lettori, abbiamo deciso di fornire delle risposte alle domande più comuni.

Per quali garanzie è valida la nuova legge?
Per capire l'oggetto della nuova legge è fondamentale capire la distinzione tra la *garanzia per i difetti di conformità* (o *garanzia legale*), da un lato, e *la garanzia di buon funzionamento*, (detta anche *garanzia convenzionale* o *garanzia commerciale*) dall'altro. La distinzione, concettualmente, è semplice, ma nella pratica non è sempre facile da applicare. La nuova legge, comunque, riguarda solo la garanzia per i difetti di conformità mentre non interviene, se non marginalmente, sulla garanzia di buon funzionamento.

Cos'è la garanzia legale?
La garanzia per i difetti di conformità, o vizi o mancanza di qualità promesse, riguarda un problema che il bene ha presentato sin dall'origine: ad esempio un processore non raggiunge la frequenza di clock promessa dal venditore. Questa garanzia si applica anche per la pubblicità (esempio: nella brochure dello scanner il produttore dichiara una certa profondità di colore che nella realtà non è rispettata). In questi casi, il consumatore può invocare la garanzia per difetto di conformità di due anni, prevista dalla nuova legge. Sono i casi in cui il contratto non è, a rigore, stato rispettato, perché è stato consegnato un bene diverso da quello previsto o non in grado comunque di svolgere le prestazioni concordate.

Cos'è la garanzia commerciale?
La garanzia di buon funzionamento (garanzia commerciale) ha, invece, un oggetto diverso: non garantisce l'assenza di vizi originari, ma il fatto che non si presentino vizi per effetto dell'uso protratto nel tempo. La garanzia di buon funzionamento, insomma, tutela il consumatore dalle usure per effetto del funzionamento.
Si tratta di una distinzione fondamentale: una stampante, ad esempio, può godere di una garanzia di conformità di due anni e di buon funzionamento di un anno. Questo significa che, se il consumatore si accorge, entro due anni, che la stampante non presenta la velocità promessa, può attivarsi. Se la stampante ha sempre funzionato correttamente ma si rompe dopo oltre un anno, la stessa deve essere riparata a spese del consumatore.
Non sempre è facile capire quando una rottura è dovuta ad un difetto di conformità o quando lo stesso bene si è semplicemente rotto per effetto dell'usura. Pensiamo ad esempio a un processore che, per un difetto di fabbricazione, non sopporta per lungo tempo il raggiungimento di una certa temperatura. Qui il bene sembra conforme al contratto sino a che non si guasta ed è proprio al momento del guasto che si può accertare la non conformità. In questo caso, il consumatore potrebbe rivalersi sul produttore anche se sono già trascorsi i termini della garanzia commerciale perché la rottura è stata determinata non dal normale uso del bene ma da un difetto di conformità.

Per quali persone si applicano le nuove garanzie?
La nuova garanzia di due anni sui difetti di conformità dei beni si applica esclusivamente ai consumatori. Non vale, in altri termini, tra imprese. Per consumatore, deve intendersi qualsiasi persona fisica che, nel contratto, agisce per scopi estranei all'attività imprenditoriale o professionale eventualmente svolta. Quindi un cliente privato con bene acquistato "a scontrino" potrà avvalersi del D.Lgs24/2002 mentre un libero professionista o imprenditore con acquisto del bene in fattura no. Ovviamente, se il difetto di conformità riguarda un bene che è stato commercializzato tra imprese per giungere ad un consumatore finale, quest'ultimo si rivolgerà al proprio rivenditore il quale potrà a sua volta rivalersi nei confronti del suo distributore.

Per quali prodotti è valida la nuova garanzia legale?
Le tutele previste dalla nuova legge si applicano a tutte le consegne di beni, che avvengano a titolo di vendita o anche fornitura, appalto, opera, sia nuovi che usati. Quindi tutte le apparecchiature informatiche sono soggette alla nuova garanzia biennale. Per i beni usati la garanzia è un po' più limitata perché la legge stabilisce che va "tenuto conto del tempo del pregresso utilizzo, limitatamente ai difetti non derivanti dall'uso normale della cosa" e, quindi, in sostanza considerata l'anzianità del prodotto.

A partire da che giorno si applicano le nuove garanzie? Ad esempio, se un consumatore acquista un notebook il 20 marzo e lo stesso gli viene consegnato il 3 aprile 2002 si può considerare operante la garanzia legale biennale?
La risposta è affermativa: la nuova legge è entrata in vigore il 23 marzo 2002. Tutti i beni che sono stati consegnati dopo tale termine, anche se il contratto è stato concluso anteriormente, godono della garanzia biennale.

Molti produttori continuano a parlare di garanzia di 1 anno quando è stata approvata la legge che estende il periodo di garanzia a due. E lecito?
Bisogna intendersi sul tipo di garanzia: per quella legale il tempo di estensione è stato portato per legge a due anni. Per quanto riguarda la garanzia commerciale, è il produttore a deciderne la validità.

In caso di guasti al prodotto in garanzia posso sempre pretendere che l'oggetto mi venga sostituito? E in questo caso a chi devo rivolgermi?
Il consumatore deve rivolgersi al negozio dove ha comperato il bene. Il guasto deve essere formalmente denunciato al venditore entro due mesi, altrimenti si può perdere il diritto alla garanzia. Per fare la denuncia, consigliamo sempre e comunque una raccomandata con ricevuta di ritorno, diretta alla sede legale del venditore. La sede legale può essere rintracciata con una tradizionale visura camerale oppure tramite la banca dati delle camere di commercio (che offre però una consultazione molto più limitata) all'indirizzo www.infoimprese.it. Nella raccomandata è sufficiente esporre sommariamente il problema che si è manifestato chiedendone la soluzione tramite i rimedi apprestati dalla legge ed indicando quale si preferisce. Tali rimedi sono la riparazione del bene o la sua sostituzione, oppure, quando impossibile, la risoluzione del contratto, che comporta che il bene venga rimesso al produttore e i soldi vengano restituiti.

Le spese correlate alla riparazione o sostituzione di un PC guasto protetto da garanzia commerciale sono a carico del consumatore?
Assolutamente no. Tutte queste soluzioni devono essere espressamente "senza spese" per il consumatore.

Il produttore si rifiuta di accordarmi la garanzia a un notebook che ho acquistato. Cosa posso fare?
Il primo passo è una formale raccomandata a ricevuta di ritorno. E dopo qualche sollecito, non si hanno comunque riscontri, bisogna procedere legalmente. Per i beni di valore inferiore ai 5 milioni di vecchie lire, attualmente 2.582,28 € in valuta corrente, la causa può essere fatta davanti al Giudice di Pace del luogo di residenza del consumatore. Si può fare a meno dell'assistenza di un legale di fiducia solo nel caso di beni di valore inferiore a 1.000.000 di vecchie lire. Se la causa, poi, si vince, solitamente le spese del giudizio e gli onorari del proprio avvocato vengono addossati dal Giudice al venditore, ma di questo non c'è mai la garanzia assoluta. ■

a cura di Tiziano Solignani avvocato in Modena

Mi farebbe un'autografo digitale?

Da qualche mese sono in vigore nuove forme di *firma elettronica*. Con il decreto legislativo 23 gennaio 2002, n. 10, è stata infatti attuata anche nel nostro paese la direttiva dell'Unione Europea 1999/93/CE, che impone a tutti gli Stati membri di adottare legislazioni uniformi in materia, con lo scopo di rendere più chiari gli scambi e le comunicazioni all'interno della Comunità.
L'Italia aveva già una propria firma elettronica, (implementata ed utilizzabile), la cosiddetta *firma AIPA*. Con la nuova legge, sono stati riconosciuti, accanto al vecchio tipo, due nuove forme di firma elettronica. Le firme elettroniche attualmente esistenti sono pertanto tre: la *firma elettronica* tout court (o *firma leggera*), la *firma elettronica avanzata* e la firma *digitale pesante* o *avanzata* che corrisponde alla vecchia firma AIPA. Ovviamente, le tre forme di sottoscrizione elettronica si distinguono tra loro per modalità di apposizione e, conseguentemente, per il grado di sicurezza che sono in grado di offrire.

La firma digitale si fa in tre

1) La firma elettronica pura e semplice, la più debole di tutte, consiste per la legge in un "insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica". Si tratta, appunto, della forma più blanda di sottoscrizione elettronica, tanto che viene detta anche firma leggera, firma debole, firma "non AIPA". Si parla di firma debole quando, ad esempio, per accedere a un determinato documento è necessario inserire un username e una password o anche semplicemente un PIN. Si tratta quindi di un tipo di firma già diffusa nella pratica anche prima dell'attuazione della direttiva UE che viene ora espressamente riconosciuta e qualificata dalla legge italiana.
2) La *firma elettronica avanzata* è quella "ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente identificati". Praticamente è la firma apposta a quei documenti che sono stati, ad esempio, criptati con programmi appositi, tra cui il più famoso è sicuramente il PGP (Pretty Good Privacy) ma senza l'utilizzo di apparati hardware tipo smartcard. In questo caso, dal punto di vista tecnico, c'è un certo grado di sicurezza circa l'attribuzione della paternità del documento e la sua integrità, che cresce parallelamente alla complessità del software impiegato. Si tratta, insomma, di una firma sicuramente più affidabile di quella elettronica pura e semplice, anche se non la più sicura in assoluto.
3) La *firma digitale avanzata*, infatti, che offre maggiori sicurezze in assoluto è quella attualmente detta pesante o firma AIPA. Si tratta appunto della firma che era già prevista in Italia, in forza del DPR 445/2000 e che è stata solo parzialmente modificata dall'attuazione della direttiva UE, che ne ha chiarito l'efficacia. È la sottoscrizione che si appone tramite l'utilizzo di dispositivi hardware e cioè di lettori di *smartcard* che leggono il certificato contenuto nella carta. Questa tecnica garantisce il più alto grado di sicurezza possibile circa la provenienza del documento da chi l'ha sottoscritto e la sua integrità.

L'efficacia legale

Per quanto riguarda, l'efficacia dei tre tipi di firma elettronica, bisogna distinguere tra firma leggera, da un lato, e, dall'altro, tra firma avanzata apposta mediante certificati avanzati e tramite l'utilizzo di smartcard.
Circa la firma elettronica leggera, la nuova legge non è per la verità molto chiara sul "valore" legale del documento digitale.
Quest'ultimo viene considerato come un documento scritto, anche se non è fisicamente esistente su carta.
La sua attendibilità viene valutata dal giudice come per qualsiasi altro mezzo di prova tenendo solo presente, genericamente, le sue "caratteristiche oggettive di qualità e di sicurezza". Da questo punto di vista, pertanto, non si può prevedere quale sarà, in caso di contestazioni, il valore riconosciuto a un documento sottoscritto in questo modo. Per le questioni dove la sicurezza è fondamentale la firma elettronica leggera non può essere utilizzata.
Le cose sono molto più chiare, invece, per la firma digitale avanzata (firma pesante o AIPA). I documenti "chiusi" con questa firma fanno piena prova, fino a "querela di falso", della provenienza delle dichiarazioni da chi li ha sottoscritti. Di fatto è assimilabile una scrittura privata riconosciuta, un documento come quello che si farebbe davanti ad un pubblico ufficiale che attesta che la sottoscrizione è stata apposta da chi ne appare come l'autore, in modo che non potrà mai più essere contestata la paternità del documento.
L'affidabilità è quindi massima. L'unico caso è quello di dimostrare la falsità del certificato, cosa naturalmente assai ardua da fare.
Per quanto riguarda, infine, la firma elettronica avanzata che non sia stata apposta tramite certificati qualificati e mediante l'impiego di smartcard, la legge non dice molto sul punto per cui la sua validità è quella, sostanzialmente, della firma elettronica debole, con il vantaggio di garantire, dal punto di vista tecnico, maggiore sicurezza, che però dovrà essere illustrata (e spiegata) al giudice il quale rimane sempre libero di valutare il documento come meglio crede.
Concludendo, a oggi, la firma digitale più sicura è quella appunto apposta tramite smartcard e tramite un certificato qualificato, quindi la "vecchia" firma AIPA, che già esisteva nel nostro Paese prima dell' attuazione della direttiva UE. Chi intende avere risultati certi nell'impiego della firma digitale per la sottoscrizione dei propri documenti, è bene che continui ad impiegare o richiedere la vecchia firma digitale, che attualmente si chiama pesante o avanzata. ■

a cura di Tiziano Solignani avvocato in Modena

Spamming, i diritti dei navigatori

Alzi la mano chi non ha mai ricevuto, nella propria mailbox, messaggi che promettono paradisi fiscali, facili guadagni o assicurazioni di vario genere. Si tratta del fenomeno, conosciuto sin dagli albori di Internet, dello spam: la posta indesiderata o comunque non richiesta, inviata per fini commerciali. Ci sono diversi sistemi tecnici per difendersi dalla posta "non sollecitata" (ne abbiamo parlato sul numero di maggio di *PC Open*). Ma, dal punto di vista giuridico, se si riceve questo tipo di posta, che cosa si può fare?

Fare spamming è vietato da leggi diverse. Intanto esiste, come noto, la famosa legge sulla privacy 675/1996, che vieta l'utilizzo di dati quali l'indirizzo di posta elettronica senza il consenso espresso del titolare. In secondo luogo, diffondere virus, come quelli usati a volte per carpire gli indirizzi di posta elettronica, che siano atti ad alterare il funzionamento di un sistema informatico, è sanzionato dal Codice Penale. Infine, lo spam è contrario alla *netiquette*, le regole tradizionali, non giuridiche, di Internet, sulle quali vigilano, però, le Authority, che sono agenzie specializzate, in grado di intervenire direttamente contro i responsabili.

Bisogna subito fare un distinguo tra posta che proviene da mittenti di nazionalità estera e posta che è stata spedita da aziende o comunque da soggetti italiani. Oggi è molto più facile difendersi dallo spam nazionale piuttosto che da quello "d'importazione" che resta difficile da combattere. Per quanto riguarda la posta di provenienza nazionale, chi la riceve ha fondamentalmente due strumenti agili e veloci a disposizione: può innanzitutto denunciare il fatto alla *Naming* e alla *Registration Autority* italiane (www.nic.it) e può, inoltre, fare la denuncia al *Garante della Privacy*.

Contattare l'Authority

Le Authority italiane hanno poteri di intervento diretto sui server che operano nel *top level domain .it* (cioè praticamente su tutti i siti che terminano con la desinenza *.it*). A queste Authority può essere segnalato l'invio di posta indesiderata, seguendo la

procedura da loro stesse descritta alle pagine www.nic.it/NA/mailspam.html. Praticamente, si deve prendere il messaggio indesiderato che si è ricevuto e, per prima cosa, fare una copia dell'*header*, cioè dell'intestazione, quella parte del messaggio solitamente nascosta e che si può visualizzare solo attivando apposite opzioni del proprio programma di posta elettronica (per chi usa Outlook, ad esempio, basta andare nel menu *Visualizza*, *Opzioni*, e appariranno le *Intestazioni Internet*). L'inclusione delle intestazioni o header è fondamentale perché consente all'Authority di ricostruire il percorso completo del messaggio.

Una volta copiato l'header del messaggio, bisogna aprirne uno nuovo e indirizzarlo a *ABUSE@na.nic.it*, e in copia a *info@nic.it*, e "incollarci" dentro l'header (si tratta di operazioni di copia e incolla da compiere con il tasto destro del mouse). A questo punto, bisogna tornare al messaggio indesiderato, copiarne il contenuto e inserirlo nel nuovo messaggio, nel frattempo lasciato aperto, indirizzato all'Authority. Una volta copiato anche il contenuto, il messaggio potrà essere spedito. La denuncia di spam inviata in questo modo verrà pubblicata anche in una mailing list i cui archivi sono consultabili pubblicamente all'indirizzo www.nic.it/RA/servizi/listserv/abuse.html. Questi archivi sono utili da consultare perché vi si riportano molti casi di spam e chi è interessato ad approfondire il fenomeno farebbe bene a darci un'occhiata.

Contattare il Garante della privacy

La seconda strada per tutelarsi, più impegnativa ma anche più efficace, è quella di rivolgersi al Garante della privacy, l'organo istituito dalla legge sul trattamento dei dati personali. Le istruzioni e anche il modello per presentare il ricorso si trovano direttamente presso il sito del Garante, all'indirizzo www.garanteprivacy.it.

I passi da compiere sono i seguenti: innanzitutto chiedere, ai sensi dell'art. 13 della legge 675/96 sulla privacy, le informazioni sul trattamento dei dati al mittente della mail, richiedendo anche il blocco del trattamento. Se non si riceve risposta, si può presentare ricorso, in via amministrativa, al Garante, denunciando la violazione della legge sul trattamento dei dati personali. A seguito di presentazione del ricorso, il Garante si rivolge nuovamente allo spammer per chiedergli ufficialmente ancora una volta le informazioni sul trattamento dei dati e, una volta acquisite le eventuali risposte, decide circa il trattamento dei dati. Nel provvedimento il Garante può imporre una multa a carico dello spammer e a favore di chi è rimasto vittima della posta indesiderata, che in questo modo è almeno ripagato in qualche modo del tempo perso a predisporre e a seguire il ricorso. Tutto questo, ad esempio, è avvenuto in un caso, ampiamente ripreso dai siti specializzati e documentato dallo stesso protagonista su internet all'indirizzo http://www.maxkava.com/spam/spam_intro.htm, dove una società italiana è stata condannata a pagare 250 euro, direttamente nelle mani di colui che aveva ricevuto la posta indesiderata. n

E-mail, gli spammer a caccia di indirizzi

Ma come fanno gli spammer ad avere gli indirizzi di posta elettronica degli utenti di internet? Usano dei software appositi, definibili genericamente come *grabber*. In sostanza, questi applicativi scandagliano il Web alla ricerca di pagine HTML che contengano indirizzi di posta elettronica - molto semplicemente, cercando stringhe che contengano il carattere @, la *chiocciolina* tipica della posta elettronica. Inoltre, parallelamente, scandagliano i newsgroup, per carpire gli indirizzi di tutti quelli che vi scrivono. Per difendersi da questi software, alcuni utenti scrivono nei newsgroup mettendo prefissi o suffissi appositi, del tipo *antispam* o *nospam* nei loro indirizzi (che, in questo modo, diventano ad es. *antispam-mario.rossi@libero.it*), specificando poi, nel corpo del messaggio, che chi intende rispondere a loro privatamente deve togliere il prefisso. Ma anche questo stratagemma non funziona, dal momento che, ovviamente, sono stati sviluppati ulteriori tipi di grabber che contengono una lista di prefissi o suffissi tipo anti grabber e, nel prendere gli indirizzi, li rimuovono (nel nostro esempio, prendono l'indirizzo *mario.rossi@libero.it*, rimuovendo il prefisso *antispam-*). Oggigiorno, dunque, chi manda sul Web una pagina contenente il proprio indirizzo, ma soprattutto chi spedisce un messaggio ad un newsgroup, inesorabilmente si ritrova il giorno dopo almeno 3 o 4 messaggi "indesiderati". Alcune soluzioni per evitare problemi sono state illustrate sul numero scorso di *PC Open* a *pagina 30*.

a cura di Tiziano Solignani avvocato in Modena

Garanzia estesa da uno a due anni

Con il decreto legislativo 2 febbraio 2002, sono state introdotte nuove forme di tutela del consumatore in occasione di acquisti di beni, tra cui anche l'hardware, di qualsiasi tipo.
Quattro sono le novità principali del decreto:
1) È stata elevata la durata della garanzia dovuta dal venditore, che per effetto della riforma è ora di due anni.
2) Le caratteristiche del bene che il venditore deve garantire non sono solo quelle espressamente indicate o convenute, ma anche quelle suggerite dalla pubblicità del prodotto, quelle che il consumatore si attende (o richiede) dal prodotto e infine quelle che sono previste per il tipo di beni in cui rientra quello acquistato dal consumatore.
3) La scelta del rimedio da porre in atto, in caso di problemi, spetta al consumatore: è l'acquirente che decide se chiedere la riparazione, la sostituzione del bene, la risoluzione del contratto o la restituzione di parte del prezzo pagato.
4) Le garanzie, poi, si applicano anche ai beni usati e non possono nemmeno essere escluse, se non entro certi limiti, dalla volontà delle parti.

È importante specificare che la nuova legge non ha abrogato nessuna delle garanzie tradizionalmente previste per l'acquirente di un bene, ma ha solo aggiunto nuove forme di tutela. Non si può, quindi, propriamente parlare di una nuova regolamentazione, che ha sostituito la vecchia, ma di una serie di strumenti che si sono affiancati e sarà il consumatore a scegliere di quali disposizioni avvalersi, a seconda di quello che riterrà migliore nel suo caso.
Il venditore è ora responsabile del problema che si manifesta entro il termine di due anni dalla consegna del bene. Il consumatore, da parte sua, deve denunciare tempestivamente i problemi al venditore. Egli infatti non può usufruire delle garanzie se non denuncia al venditore il cosiddetto *difetto di conformità* entro due mesi.

Il difetto di conformità

In quest'ottica, i beni risultano conformi solo quando:
1) Sono idonei all'uso al quale servono abitualmente beni dello stesso tipo, tenuto conto della natura del bene e delle dichiarazioni pubbliche sulle caratteristiche specifiche dei beni fatte al riguardo dal venditore, dal produttore o dal suo rappresentante (in particolare nella pubblicità o sull'etichettatura).
2) Sono conformi alla descrizione fatta dal venditore e presentano le caratteristiche del bene che il venditore ha presentato al consumatore come campione o modello.
3) Sono idonei all'uso particolare voluto dal consumatore. Quest'ultimo è ad esempio il caso in cui il consumatore si è rivolto al venditore richiedendogli non un prodotto specifico, ma illustrando un'esigenza e chiedendo un prodotto in grado di risolverla. È il caso di un utente informatico che può andare dal proprio negoziante chiedendo una scheda video idonea per poter giocare con un certo videogame: nel caso in cui la scheda, poi, non funzioni con quel gioco, anche se non presenta nessun altro vizio o problema di funzionamento, il consumatore può ugualmente avvalersi delle garanzie e chiedere anche lo scioglimento del contratto.

I diritti del consumatore

Il consumatore ha diritto al ripristino, senza spese, della conformità del bene o a una riduzione adeguata del prezzo o alla risoluzione del contratto, che comporta la restituzione del bene a fronte del risarcimento della cifra pagata. È il consumatore che decide qual è la giusta modalità di risarcimento, salvo che il rimedio richiesto sia oggettivamente impossibile o eccessivamente oneroso.
Se, ad esempio, è troppo costoso riparare un bene, il venditore può sostituirlo senza che il consumatore possa chiedere a tutti i costi la riparazione. In ogni caso, le riparazioni o le sostituzioni devono essere effettuate entro un "congruo termine" dalla richiesta e non devono arrecare "notevoli inconvenienti" al consumatore, tenendo conto della natura del bene e dello scopo per il quale il consumatore ha acquistato il bene.
Il consumatore può richiedere una congrua riduzione del prezzo o la risoluzione del contratto ove ricorra una delle seguenti situazioni: la riparazione e la sostituzione sono impossibili o troppo onerose, il venditore non ha provveduto alla riparazione o alla sostituzione del bene entro il termine congruo o la sostituzione o la riparazione precedentemente effettuata ha dato notevoli problemi al consumatore. In sostanza, il consumatore può chiedere i soldi indietro nel caso in cui né la sostituzione né la riparazione abbiano risolto il suo problema. In caso di problemi, comunque, il consumatore almeno in un primo momento può limitarsi a denunciarli a controparte, sempre con la solita raccomandata a ricevuta di ritorno, per poi valutare il rimedio effettivo da richiedere, in caso di mancata ottemperanza da parte del venditore, insieme ad un legale di fiducia.
La denuncia non è necessaria solo se il venditore ha riconosciuto l'esistenza del difetto. La denuncia può essere fatta anche oralmente, ma ovviamente è di rigore la raccomandata a ricevuta di ritorno. Se il venditore non risponde ai solleciti e alla raccomandata, il consumatore deve decidere entro 26 mesi se fare causa al venditore o lasciar perdere. Dopodichè non avrà più la possibilità di farlo.

I beni di seconda mano

Le nuove garanzie si applicano espressamente anche ai beni di seconda mano.
Per i beni usati, la legge prescrive solamente che nel decidere circa l'applicazione delle garanzie occorre tener conto del "tempo del pregresso utilizzo, limitatamente ai difetti non derivanti dall'uso normale della cosa".
Si tratta per la verità di una disposizione non chiarissima (e quindi a discrezionalità del giudice), che sembra voler dire che si devono valutare con maggior indulgenza i beni più vecchi.
La responsabilità del venditore di beni usati può essere limitata, ma comunque non può mai essere inferiore ad un anno.
Questo, ad esempio, esclude che un bene di seconda mano possa essere venduto con la diffusa formula "as is", cioè così com'è e questo sembra eccessivo: può essere infatti un onere eccessivo per un venditore di beni usati doverli garantire per addirittura un anno dopo la vendita. n

QUANDO SI PARTE?

Il decreto legislativo contenente le disposizioni di riforma è stato pubblicato sulla Gazzetta Ufficiale il giorno 8 marzo 2002 ed è entrato in vigore 15 giorni dopo, il 23 marzo 2002. Le nuove disposizioni si applicano a tutte le vendite di beni e contratti equiparati in cui la consegna del bene avviene dopo quella data: il contratto può anche essere stato concluso prima, l'importante è che il bene sia consegnato dopo il 23. Per le disposizioni sulle *garanzie convenzionali*, è previsto che le stesse non si applichino ai prodotti immessi sul mercato prima del giorno 23 marzo 2002: in realtà si tratta di disposizioni di scarsa importanza. La data che bisogna tenere presente è comunque il 23 marzo 2002. Per tutti i beni consegnati dopo quella data valgono le nuove garanzie.

IVA, come cambia l'imposta per il commercio elettronico

All'ultima riunione dell'Ecofin, l'organo che riunisce tutti i ministri economici degli Stati membri dell'Unione Europea, è stato varato il progetto di nuova direttiva in materia di regime IVA per il commercio elettronico. La principale novità della direttiva è che la prestazione viene tassata presso il committente, cioè presso l'acquirente, sia egli consumatore finale o altro imprenditore. In sostanza si applica il regime IVA previsto nel Paese in cui risiede il consumatore finale, con la precisazione che se questi risiede in uno Stato non facente parte dell'Unione l'operazione non è imponibile.
La questione dell'IVA sulle transazioni internazionali è sempre stata problematica, tant'è vero che la disciplina europea attuale è sempre stata qualificata come *transitoria* (ma nonostante questo va avanti da una decina d'anni). Nel caso del commercio elettronico, le tradizionali difficoltà sono state amplificate: infatti in molti casi manca la consegna materiale del bene compravenduto, come ad esempio nell'ipotesi in cui si acquista un software scaricandolo, tramite una procedura di download, dal sito del produttore. Questo, ovviamente, rende molto difficile il controllo da parte delle Amministrazioni fiscali dei vari Stati. Proprio queste ultime, che guardano da tempo al commercio elettronico come un preoccupante buco nero per evasioni ed elusioni, sono state le maggiori promotrici di un intervento legislativo europeo. La nuova direttiva, in teoria, dovrebbe costituire l'attuazione dei principi posti in materia di e-commerce dall'OCSE nel vertice di Ottawa del 1998, che dovrebbero consistere nella neutralità, efficienza, flessibilità, certezza e semplicità della tassazione. In realtà dovrebbe servire anche a garantire condizioni di parità per tutti gli imprenditori che intendono offrire beni o servizi a consumatori che risiedono nel territorio dell'Unione Europea.
La direttiva, in ogni caso, riguarderà sia le transazioni tra gli operatori commerciali (il cosiddetto *business to business, B2B*) sia quelle con i consumatori (il *business to consumer, B2C*). Le operazioni interessate saranno le seguenti:
• Progettazione, realizzazione e manutenzione di siti Web.
• Contratti di Web hosting.
• Fornitura di programmi e loro aggiornamento.
• Cessione di immagini, di musica, di film e di giochi.
• Programmi politici, culturali, sportivi, scientifici e di divertimento.
• Formazione a distanza.
• Accesso a banche dati.
Sono esclusi, invece, i servizi relativi a radio e televisione.
Il nuovo meccanismo garantisce alle imprese condizioni paritarie nel momento in cui vendono all'interno dell'Unione e condizioni addirittura di vantaggio nel momento in cui operano all'esterno. Il tutto anche a discapito del consumatore. Infatti, ad esempio, il consumatore italiano che oggi può rivolgersi alle imprese di quegli Stati in cui non è prevista l'IVA (o è prevista con una aliquota ridotta), trovando magari gli stessi beni a costo inferiore, non potrà più farlo quando verrà attuata la nuova direttiva, perché a qualsiasi operazione che si terrà in Italia sarà applicato il regime italiano, indipendentemente dalla nazionalità del produttore. Il produttore, poi, quando andrà a vendere a un consumatore, ad esempio, statunitense non sarà soggetto ad IVA con la conseguenza che il bene costerà meno e sarà più allettante per il consumatore residente in un Paese che non è membro dell'Unione.
Per attuare questo meccanismo, tutti gli operatori economici dovranno *identificarsi* e cioè in qualche modo avere una base all'interno di uno degli Stati membri dell'Unione. Così un operatore statunitense per poter vendere in Italia, e in tutti gli altri Stati membri, potrà stabilirsi ad esempio in Germania. In questo modo, in caso di transazioni tra operatori economici (B2B) fiscalmente identificati in Stati diversi, l'operazione sarà imponibile presso il committente il quale dovrà autoliquidarsi l'imposta con una procedura detta di *reverse charge*. In caso, invece, di operazione verso il consumatore finale (B2C), l'operazione risulterà sempre imponibile presso il committente, ma verrà fatturata direttamente con imposta da parte del fornitore, che dovrà identificarsi anche nello Stato del consumatore finale.
La direttiva dovrebbe entrare in vigore nel luglio 2003. Essa ha espressamente un'efficacia limitata nel tempo, di tre anni, sino a giugno 2006. È previsto che la sua efficacia possa essere estesa anche oltre, finendo magari per essere una disciplina transitoria che, come quella attuale, dura per molto più tempo del previsto.
Per tale estensione è necessaria, comunque, una approvazione all'unanimità.
È evidente che provvedimenti di questo tipo si basano su equilibri politici, anche internazionali e intercontinentali molto delicati, e saranno molto importanti le reazioni al nuovo regime che verranno dagli Stati Uniti e dalle altre grandi aree economiche del mondo, specialmente in considerazione del fatto che il nuovo sistema prevede sostanzialmente un'esenzione per le imprese dell'Unione che forniscono beni o servizi a Paesi che non sono membri della Comunità. n

La nuova direttiva

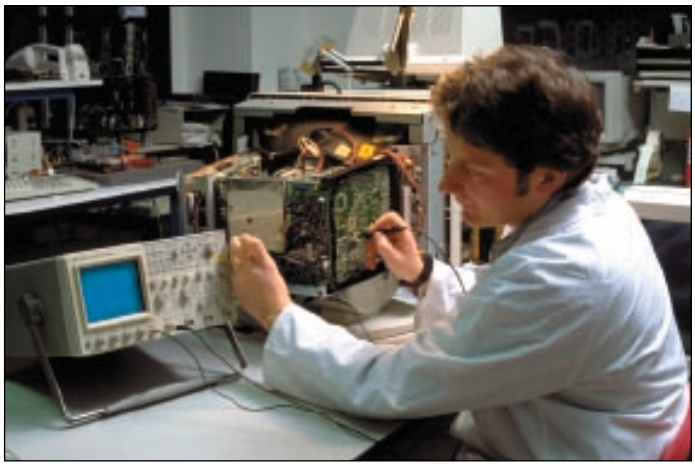
COSA CAMBIA
Nella vendita di beni fra diversi stati effettuati tramite e-commerce, si applicherà l'IVA del Paese nel quale risiede l'acquirente. Questo significa che il consumatore italiano che compra un software via e-commerce dovrà sempre aggiungere il 20% di IVA.

I TEMPI DI ATTUAZIONE
La direttiva dovrebbe entrare in vigore nel luglio 2003 con validità triennale.

LE TRANSAZIONI COINVOLTE
1) progettazione, realizzazione e manutenzione di siti Web;
2) contratti di Web hosting;
3) fornitura di programmi e loro aggiornamento;
4) cessione di immagini, di musica, di film e di giochi;
5) programmi politici, culturali, sportivi, scientifici e di divertimento;
6) formazione a distanza;
7) accesso a banche dati.

Assistenza post vendita, i diritti dell'utente informatico

Sempre più determinante, per l'acquisto di un computer o di una stampante ma anche per la sottoscrizione di un abbonamento ad un servizio, è la promessa di assistenza che viene fatta dal venditore al potenziale acquirente per il periodo successivo all'acquisto. L'hardware, infatti, è noto per essere soggetto a non infrequenti problemi o comunque per essere semplicemente ostico da installare, configurare, usare. Lo stesso dicasi, sul versante dei servizi, per le connessioni telematiche ad esempio. Ma qual è la validità legale delle promesse fatte, in materia, dal venditore?



Garanzia e assistenza

È meglio chiarire, innanzitutto, il concetto di assistenza, che va tenuta distinta dalle garanzie vere e proprie di cui gode il consumatore. L'assistenza è una ulteriore forma di "servizio" cui è tenuto il venditore verso il consumatore ed è diversa dalle garanzie in senso stretto. In primo luogo, infatti, esistono per l'acquirente o il sottoscrittore le garanzie vere e proprie. La cosa o il servizio che viene sottoscritto deve essere immune da vizi di origine e deve presentare le caratteristiche indicate al momento dell'acquisto: il processore deve essere del tipo indicato, la memoria della quantità prevista, la linea deve avere la velocità richiesta e così via. Oltre a queste tutele di base, il fornitore quasi sempre, oltre ad assicurare la bontà del prodotto al momento dell'acquisto, garantisce anche che questa si mantenga nel tempo, per un periodo solitamente di uno o due anni. Questa è la *garanzia* più conosciuta nella pratica, detta dai giuristi *di buon funzionamento*, con la quale il consumatore è tutelato in caso di rotture successive dell'hardware, ovviamente solo entro il periodo specificato e alle condizioni previste dalla garanzia stessa. Questa garanzia non è obbligatoria per legge ma esiste solo quando *concessa* dal venditore. In questo contesto, l'assistenza è una cosa diversa e presuppone un prodotto o servizio che funziona a norma di contratto. Essa è un servizio ulteriore al quale il venditore si obbliga, tanto che spesso, nelle vendite di grandi partite di hardware, il contratto di assistenza esiste fisicamente su carta ed è separato da quello di vendita. Come la garanzia di buon funzionamento, l'assistenza è un diritto del consumatore solo se espressamente prevista nel contratto o nelle sue condizioni generali. In realtà, quando il venditore si obbliga all'assistenza, il contratto che viene concluso dalle parti è un contratto misto di vendita e fornitura di servizi. Quando sottoscrive l'abbonamento a un servizio, il consumatore non paga solo il costo del bene ma anche dell'assistenza sul bene suddetto. A sostanziale parità di prodotti, poi, molti rivenditori o produttori si fanno concorrenza sui servizi di assistenza la cui offerta diventa così strategica per rimanere sul mercato.

L'obbligo da parte del venditore

Ad ogni modo, quello che un venditore promette in sede di vendita, è per lui obbligatorio. In altri termini, l'assistenza, una volta promessa dal venditore o fornitore, deve essere erogata. È insomma un diritto per il consumatore ricevere l'assistenza promessa al momento dell'acquisto, sia essa telefonica, on site, via e-mail, via telefono o in ognuna delle svariatissime forme in cui può essere configurata. Se il consumatore non riceve l'assistenza promessa, può chiedere il risarcimento del danno e, se la mancanza è di fondamentale importanza nell'economia del contratto, può chiederne anche la risoluzione, restituendo l'oggetto acquistato ed avendo indietro i soldi.

In caso di inadempienze del fornitore

Al di là delle forme in cui viene erogata l'assistenza, e cioè sia che la stessa sia erogata via numero verde, posta elettronica, on site o diversamente, è opportuno che il consumatore smetta di telefonare o inviare e-mail, destinate a perdersi in quelli che talvolta sono veri e propri "buchi neri" dei reclami, ma ricorra ad una tradizionale raccomandata a ricevuta di ritorno.
La cosa migliore da fare, infatti, è quella di provare, magari per qualche giorno, a rivolgersi al servizio di assistenza nelle forme previste, ma poi, in caso di ritardi che superano la settimana, bisogna attivarsi diversamente. La raccomandata va inviata alla sede legale, e non solo amministrativa che può essere diversa, del fornitore. Per conoscere la sede legale del fornitore, si può far capo quasi sempre al relativo sito Internet oppure, in mancanza ma anche per maggior sicurezza, agli sportelli della Camera di Commercio della propria provincia.
Nella lettera, oltre a lamentare la mancata erogazione del servizio di assistenza, occorre prospettare di adire le vie legali in caso lo stesso non sia ripristinato ed erogato entro un certo termine.

Meglio usare i pagamenti a rate

Nel caso di acquisto di grosse partite hardware, ma anche in caso di sottoscrizione di abbonamenti per la fornitura di servizio, come ad esempio quelli di connessione alla rete Internet, è sempre consigliabile pagare a rate o comunque con scadenze periodiche: in caso di prestazioni assai deludenti del servizio assistenza, si può persino legittimamente interrompere il pagamento.
Anche in questo caso meglio inviare una preventiva raccomandata a ricevuta di ritorno. In questa raccomandata il consumatore deve spiegare che il pagamento viene sospeso solo ed esclusivamente per mancanza erogazione del servizio di assistenza di cui costituisce il corrispettivo e che il contratto, in difetto di ripresa dell'erogazione del servizio entro 15 giorni, dovrà intendersi risolto.

Tiziano Solignani

L'assistenza in pillole

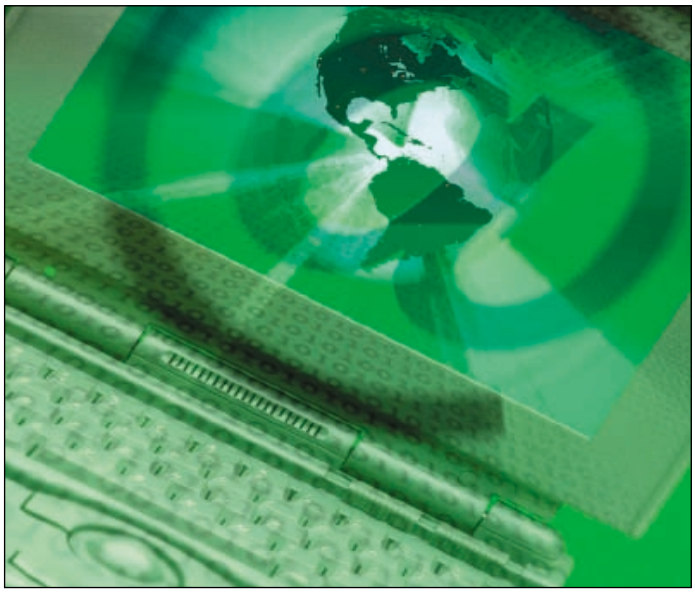
- L'assistenza è un servizio diverso dalla garanzia e concesso dal venditore (non c'è obbligo).
- Deve essere siglato un contratto spesso separato da quello di vendita.
- In questo contratto devono essere definiti i termini di erogazione. In caso di inadempienza, il consumatore può chiedere il risarcimento del danno e la risoluzione del contratto (bisogna mandare una raccomandata con ricevuta di ritorno alla sede legale).
- Nel caso di acquisto di grosse partite hardware è consigliabile pagare a rate o comunque con scadenze periodiche (si può legittimamente interrompere il pagamento).

Il commercio elettronico tra fisco, tasse ed elusioni

Il commercio elettronico pone, tra gli altri, problemi di ordine fiscale, soprattutto in considerazione delle elusioni, più o meno legittime, che ne possono derivare. Infatti, quando la compravendita di beni o servizi avviene secondo i criteri tradizionali, di solito compratore e venditore appartengono al medesimo Stato, e dunque soggiacciono alla medesima disciplina fiscale. Il commercio tradizionale poi presuppone la presenza di intermediari (quali banche o commercianti) che assicurano trasparenza all'operazione e garantiscono il pagamento delle imposte.

Cosa cambia su Internet

Quando il commercio si trasferisce su Internet le cose cambiano. In primo luogo, chi offre un bene o un servizio per via elettronica può scegliere liberamente lo Stato in cui dislocare la propria attività: va da sé che, potendo, verrà scelto lo Stato che offre una disciplina fiscale più permissiva. Inoltre, lo scambio di beni o servizi tramite Internet consente di fare a meno di intermediari: lo scambio avviene direttamente tra produttore e consumatore, con conseguente possibilità di eludere completamente la normativa fiscale. Non può dunque stupire che, da qualche anno, si sia intensificato il dibattito per garantire l'applicazione della legislazione fiscale e doganale alle operazioni commerciali concluse per via elettronica. Per esempio, nell'ottobre 1998 l'OCSE ha tra l'altro adottato un rapporto, sottoscritto da 30 Stati, che si fonda sul principio per cui le regole del commercio elettronico devono fondarsi sugli stessi principi fiscali che regolano il commercio tradizionale. In altre parole, per risolvere le questioni fiscali derivanti dal commercio elettronico, non sono necessarie regole giuridiche nuove e in particolare nuove imposte, ma è sufficiente applicare le imposte e le regole già esistenti, eventualmente adattandole. Per quanto riguarda specificamente l'IVA, l'OCSE già nel 1997 ha proposto che il bene o il servizio sia soggetto all'imposta vigente nel Paese in cui quel bene o quel servizio è consumato, e ciò a prescindere dal luogo di produzione o in cui si trova il venditore, e anche dal luogo in cui si trova il consumatore nel momento in cui è conclusa la transazione. Ciò vuol dire che se un italiano compra tramite Internet un CD negli USA, sul bene deve essere pagata l'IVA. Questa regola è di agevole applicazione nel caso in cui l'e-commerce riguardi merce ordinata elettronicamente ma consegnata con sistemi tradizionali (per esempio, per posta): in casi come questi, l'acquisto è sottoposto al pagamento dei diritti doganali al momento del passaggio della frontiera. Tuttavia, la stessa regola è insufficiente quando l'oggetto della transazione sia un bene non consumabile o un servizio "virtuale" (esempio il download di brani musicali o una consulenza via e-mail).



Le direttive dell'Unione Europea

Per risolvere questo problema, un documento approvato dalla Ue nel giugno 1998 qualifica come prestazione di servizio, e dunque come soggetto ad IVA se il servizio è consumato nel territorio dell'Unione, ogni transazione che abbia a che fare con un bene virtuale. Per arginare l'evasione dell'imposta, la stessa Commissione ha proposto, nel giugno 2000, che ogni società extracomunitaria, che venda servizi nel territorio dell'Unione Europea per oltre 200.000.000 di lire, debba necessariamente aprire una propria sede nel territorio dell'Unione. Nonostante i risultati fin qui raggiunti, comunque ci sono ancora diversi punti deboli e su questo versante, è inevitabile che le autorità saranno seriamente impegnate nel corso degli anni a venire.

Stefano Chiusolo

Con l'e-commerce si può evadere l'IVA

Il commercio elettronico consente, ad operatori con pochi scrupoli, di eludere o addirittura di evadere le imposte. Per esempio, chi offre beni o servizi tramite Internet può facilmente dislocare la propria attività in uno Stato che offre una disciplina fiscale permissiva; inoltre, il commercio elettronico avviene direttamente tra produttore e consumatore, senza intermediari quali banche o commercianti che svolgono un importante ruolo per garantire la trasparenza fiscale e il pagamento delle imposte. Per questo motivo, autorità come l'OCSE o l'Unione Europea hanno approvato risoluzioni o avanzato proposte per disciplinare il regime fiscale delle transazioni elettroniche.
I principi che hanno ispirato tali risoluzioni sono i seguenti:

- Il commercio elettronico si deve fondare sugli stessi principi fiscali del commercio tradizionale, eventualmente adattati alle nuove problematiche: non sono necessarie nuove regole né nuove imposte.
- Per quanto riguarda l'IVA, è necessario che il bene o il servizio sia soggetto all'imposta vigente nel Paese in cui lo stesso è consumato.
- Se la transazione elettronica ha ad oggetto un bene reale consegnato con mezzi tradizionali, l'acquisto deve essere sottoposto al pagamento dei diritti doganali.
- Se la transazione elettronica ha come oggetto un bene virtuale (brano musicale, consulenza), l'oggetto della transazione deve essere qualificato come servizio e, se consumato all'interno dell'Unione Europea, deve essere assoggettato ad IVA anche se fornito da un soggetto extracomunitario.

In ogni caso, queste regole non sono ancora in grado di arginare l'evasione fiscale, resa possibile soprattutto dall'anonimato delle transazioni via Internet e dalla difficoltà dei controlli fiscali. Questo è il versante su cui le autorità e i Governi dovranno impegnarsi nei prossimi anni.

a cura di Tiziano Solignani avvocato in Modena www.solignani.it

I diritti di chi compra un personal computer

Quali sono i diritti di chi acquista un personal computer? La risposta cambia, in primo luogo, a seconda del modo in cui è avvenuta l'acquisto.
Bisogna infatti distinguere tra transazioni tradizionali, cioè effettuate personalmente dal consumatore nei negozi, e acquisti a distanza, via posta o tramite Internet. C'è infatti un gruppo di garanzie di base che si applica in qualsiasi caso, mentre per chi acquista a distanza sono previste ulteriori e specifiche garanzie.

Le garanzie di ogni consumatore

Il consumatore, gode sempre e comunque di tre garanzie: quella contro i vizi occulti, quella contro la mancanza di qualità promesse e quella di buon funzionamento.
1) Garanzia contro i *vizi occulti*. Il venditore deve, innanzitutto, garantire che il bene, appena venduto, funzioni e non presenti vizi che ne diminuiscano il valore o comunque impediscano in tutto o in parte che possa essere utile. Se, quindi, una scheda, un monitor, una tastiera, un mouse o qualunque altro componente del computer appena acquistato non funzionano, questa è la garanzia da far valere. Il difetto deve essere denunciato al venditore entro 8 giorni dalla scoperta. È indispensabile utilizzare per la denuncia la raccomandata a ricevuta di ritorno. Una volta fatta la denuncia, se il venditore non adempie, è necessario agire in giudizio contro di lui entro un anno, altrimenti si perde ogni diritto.
2) Garanzia delle *qualità promesse*. È quella che si può far valere quando, ad esempio, viene venduto per modem con velocità di 28.800 un modem che, in realtà, marcia solo a 14.400; oppure un Pentium 3 è stato spacciato dal venditore per un Pentium 4. La differenza rispetto alla garanzia precedente sta nel fatto che il bene venduto non presenta in realtà nessun difetto. Però non presenta le caratteristiche concordate. Anche in questo caso, occorre denunciare la scoperta entro 8 giorni per poi agire, se è il caso, entro un anno dalla denuncia.
3) Garanzia di *buon funzionamento*. Questa è la garanzia per eccellenza, quella alla quale corre automaticamente il pensiero quando si parla di "garanzia" senza ulteriori specifiche.
Serve a proteggere dai guasti che si verificano in un bene che, pur essendo in piena regola al momento dell'acquisto, si deteriora nel tempo. Mentre le prime due forme di garanzia sussistono sempre e comunque, quest'ultima si ha solo quando è stata espressamente rilasciata dal venditore. Solitamente, nella garanzia stessa sono previsti i termini e i modi per farla valere, che spesso prevedono la spedizione di un tagliando alla casa produttrice. In mancanza, la denuncia del guasto deve avvenire entro 30 giorni dalla scoperta e l'azione contro il venditore inadempiente deve poi iniziare entro i 6 mesi successivi.

Le garanzie dei consumatori on line

Il nostro Paese ha dato attuazione alla direttiva dell'Unione Europea, in materia di protezione del consumatore nei contratti a distanza. Esisteva già una disciplina di tutela per questo tipo di contratti, contenuta nel Decreto Legislativo 15 gennaio 1992, n. 50. La nuova legge prevede che, in futuro, le due normative dovranno essere "fuse" in un testo unico di tutela del consumatore a distanza. Fino a che ciò non avverrà, continueranno ad applicarsi entrambe le due leggi, scegliendo volta per volta la disposizione più favorevole al consumatore. La ragione che giustifica l'applicazione di tutele maggiori per chi acquista, ad esempio, via Internet risiede nel fatto che, nella contrattazione a distanza, l'acquirente non può visionare il bene come nei contratti stipulati a contatto diretto con il venditore, così come quando si entra in un tradizionale negozio o centro commerciale. Per tali motivi, si riconosce un diritto di recesso dal contratto, esercitabile senza che sia dovuta alcuna motivazione e quindi, evidentemente, anche solo perché il bene che ha acquistato, una volta che l'ha visto davvero, non gli è piaciuto. Il consumatore a distanza, dunque, ha quasi sempre, salvo alcune eccezioni specificamente previste, il diritto di recedere dal contratto entro un certo termine, cioè di restituire il bene e riavere indietro i soldi. Il diritto di recesso si esercita inviando nel termine previsto dalla legge una raccomandata con avviso di ricevimento alla sede legale del fornitore.
Sono previste alcune eccezioni al recesso, tra cui 1) Beni confezionati su misura o chiaramente personalizzati che, per loro natura, non possono essere rispediti o rischiano di deteriorarsi o alterarsi rapidamente. 2) Prodotti audiovisivi o software informatici sigillati che siano stati aperti dal consumatore oppure giornali, periodici o riviste.

E se il venditore non fa nulla?

Come si vede, quindi, la legge italiana in materia di tutela dell'acquirente è completa e rigorosa. I problemi, però, possono nascere ugualmente quando il venditore chiamato in garanzia non ripara il computer oppure non restituisce il prezzo pagato; in tal caso, non resta altro che iniziare una causa civile della probabile durata minima di quattro o cinque anni, nel corso della quale il compratore dovrà anticipare ogni spesa. In questi casi, ovviamente, si decide di andare avanti per lo piú quando la cosa è divenuta una questione di principio, salvo che l'hardware acquistato non abbia effettivamente un costo notevole, mentre in tutti gli altri si preferisce, pur avendo sostanzialmente ragione, abbandonare. Per questo motivo è sempre meglio cercare l'appoggio e il sostegno delle associazioni dei consumatori. n

Tiziano Solignani

Cosa fare quando qualcosa non va

1 Scrivere una lettera raccomandata con ricevuta di ritorno diretta alla sede legale del venditore. In caso di vizio o mancanza di qualità promesse o rottura, bisogna fare presenti i vizi o le caratteristiche mancanti e chiederne al venditore l'eliminazione entro un certo termine dal ricevimento della lettera, specificando che in caso contrario si procederà giudizialmente per ottenere il rispetto delle garanzie di legge.

2 Nel caso di recesso, bisogna restituire il bene (meglio se con posta celere), con una lettera di accompagnamento in cui si dichiara appunto di esercitare il diritto di recesso e che si rimane in attesa della restituzione di quanto pagato. In tutti questi casi, bisogna scordarsi delle telefonate, fax o delle comunicazioni via e-mail o posta ordinaria. Meglio fare subito una raccomandata, che comunque non preclude alla sistemazione bonaria della vicenda. Per quanto riguarda il recesso, il termine per l'esercizio dello stesso è di dieci giorni lavorativi, nel caso in cui il consumatore sia stato correttamente informato della possibilità di esercitarlo. In caso di mancata comunicazione al consumatore da parte del venditore il diritto di recesso è esercitabile entro 3 mesi.

3 Una volta inviata la raccomandata, se il venditore non fa quello che dovrebbe fare, bisogna valutare se fare una causa civile, tenendo presente che ci sono ancora una volta dei termini, diversi a seconda del tipo di garanzia, trascorsi i quali non si può più procedere.