# ICT E DIRITTO

## Rubrica a cura di

**Antonio Piva e David D'Agostini**

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

# Le comunicazioni elettroniche non sollecitate

### Introduzione

Chiunque possiede una casella di posta elettronica e quotidianamente riceve un discreto numero di messaggi dal contenuto pubblicitario conosce bene in prima persona il fenomeno dello *spam* (noto anche come *junk-mail*).
Questo vocabolo dalla chiara accezione spregiativa (acronimo di *Send Phenomenal Amounts of Mail*, nonché marca americana di carne in scatola) viene utilizzato per indicare l'invio massivo e spesso indiscriminato di comunicazioni elettroniche non desiderate; come noto si tratta di una pratica commerciale sviluppatasi negli anni '80, che ora ha raggiunto livelli preoccupanti se si pensa che nel 2003 oltre la metà del traffico e-mail era composto da *spam* e la percentuale risulta in crescita.
È solo il caso di accennare alle potenzialità lesive di tale fenomeno a danno degli utenti di Internet, non solo in riferimento alla riservatezza (configurandosi come un'intrusione nella vita privata di un individuo), ma anche sotto il profilo economico: appare evidente, infatti, che il destinatario deve sopportare, suo malgrado, le spese di connessione per la durata necessaria a scaricare le *e-mail* indesiderate, oltre al tempo perso per visionare ed eliminare tali messaggi.
Da ultimi, ma non per importanza, si pongono i problemi di natura tecnica e, naturalmente, i costi connessi alla loro risoluzione (che ancora una volta sono a carico dei navigatori): infatti per far transitare queste enormi quantità di dati elettronici è necessario aumentare da un lato la larghezza di banda, dall'altro la capacità di archiviazione dei server di posta elettronica (in particolare dei POP3 che ricevono i messaggi).
Il problema non è di poco conto: su scala mondiale i costi diretti e indiretti ammontano ad oltre 10 miliardi di euro all'anno con ingenti danni per gli utenti (la cui spesa pro capite è stimata in 30 €) e conseguente perdite di produttività per le imprese, derivanti dal calo di fiducia del popolo della rete, condizione indispensabile per il buon successo del commercio elettronico.
Inoltre, come se non bastasse, ultimamente si registra lo sviluppo di una variante di *spam* ancora più invasiva, lo SPIM (*Spam over Istant Messaging*), ossia la pubblicità tramite messaggi telefonici del tipo MMS (*Multimedia Messaging Service*) o SMS (*Short Message Service*).
Per le ragioni illustrate, l'invio di comunicazioni commerciali indesiderate è stato oggetto di provvedimenti, non solo normativi, tra i quali si ricorda la direttiva comunitaria 2002/58/CE (recepita dall'Italia in alcune norme del Codice in materia di protezione dei dati personali) e la recente Comunicazione COM(2004)28, in cui si individuano una serie di azioni di contrasto a carattere prevalentemente giuridico e tecnico.

### Aspetti tecnici

La lotta allo *spam* è stata combattuta in primo luogo con l'ausilio di diversi mezzi tecnici, suggeriti dalla stessa comunità Internet[1]; quest'ultima, dal canto suo, ha sempre considerato l'invio di messaggi di posta elettronica

[1] Il gruppo di lavoro anti-spam del RIPE (reti IP europee) è attivo sin dal 1998 (cfr. il documento "*Good Practice for combating Unsolicited Bulk Email*" pubblicato sul sito RIPE (http://www.ripe.net).

non sollecitati come una violazione delle norme di *Netiquette*, nonché dei principi di uso corretto delle risorse di rete enunciati nei documenti RFC1855 e RFC2635.
Un ruolo fondamentale viene naturalmente riconosciuto ai fornitori d'accesso (*Internet Service Provider*); la loro organizzazione in una rete denominata "*The Mail Abuse Prevention System*" ha portato alla formazione delle liste nere *Realtime Blackhole Lists* (RBL) che, controllando migliaia di router e di server di posta elettronica, permettono loro d'informarsi reciprocamente sulle operazioni di *spamming* di cui sono oggetto e di mettere all'indice gli indirizzi IP e nomi di dominio conosciuti per essere all'origine di pubblicità indesiderata, bloccando automaticamente l'invio di messaggi provenienti da uno *spammer* identificato e dal *provider* che lo ospita.
Gli stessi prestatori di servizi di comunicazione elettronica, ed anche gli utenti finali, cercano inoltre di tutelarsi installando appositi *software* di filtraggio. Tuttavia questi dispositivi di filtraggio possono, per errore, lasciare passare alcuni messaggi di *spam* (falsi negativi), ma soprattutto rischiano di bloccare indebitamente i messaggi leciti (falsi positivi), caso ben più grave che configura una responsabilità a carico degli ISP (*Internet Service Provider*). Il mittente o il destinatario potrebbero intraprendere un'azione giudiziaria nei loro confronti.
Per tale ragione alcuni *provider* propongono il servizio di filtraggio come opzione commerciale e chiedono all'utente l'autorizzazione espressa ad attivarlo.
Particolare attenzione meritano anche i cosiddetti "*relay aperti*", ossia i server SMTP (*Simple Mail Transfer Protocol)* (attraverso i quali si inviano i messaggi) che sono configurati in modo da essere utilizzati da chiunque, anche da chi non è riconosciuto come utente di tale *provider*.
Una volta quasi tutti i relay venivano lasciati aperti per favorire le trasmissioni, e ciò creava una condizione ottimale per l'invio di comunicazioni indesiderate; semplici misure preventive da parte degli amministratori di sistema potrebbero consentire una sostanziale riduzione delle pratiche abusive in questo settore (nelle ultime distribuzioni di Linux gli SMTP che possono essere installati di default hanno i relay chiusi). I gestori di server di posta elettronica, pertanto, devono provvedere a un'adeguata protezione dei loro server impedendo il funzionamento in modalità "relay aperto", salvo sia assolutamente necessario.

## Il quadro normativo

In Italia la norma sulle comunicazioni indesiderate dettata dalla Direttiva 58/2002/CE è stata recepita nell'art.130 del Codice della privacy, il quale prevede che l'uso della posta elettronica per l'invio di materiale pubblicitario (o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale) sia consentito solo con il previo consenso dell'interessato, secondo un principio che prende il nome di "*opt-in*".
Questa regola vale anche per i sistemi automatizzati di chiamata senza l'intervento di un operatore, i telefax e i messaggi *Mms*, *Sms* o di altro tipo.
La regola dell'*opt-in* conosce un'importante eccezione: viene ammesso, infatti, che il titolare del trattamento utilizzi l'indirizzo di posta elettronica conferito dall'interessato nel contesto di una precedente vendita, per l'invio di comunicazioni inerenti a prodotti o servizi analoghi a quelli già acquistati; comunque il destinatario della comunicazione dev'essere informato della possibilità di opporsi a ulteriori messaggi in qualsiasi momento e in modo semplice e gratuito (procedura di "*unsubscribe*"). In quest'ultima ipotesi vige la regola opposta di "*opt-out*", vale a dire del rifiuto a posteriori.
In ogni caso, nel rispetto del principio di trasparenza, al mittente è sempre vietato camuffare o celare la propria identità; inoltre il titolare è tenuto a fornire indicazioni sul recapito presso cui il destinatario potrà esercitare i propri diritti di opposizione a ulteriori invii, oltre che di accesso (per esempio chi riceve un'e-mail pubblicitaria può chiedere da dove è stato preso il suo indirizzo).
In caso di reiterata violazione delle regole in tema di comunicazioni elettroniche appena illustrate, il Garante può prescrivere ai fornitori di servizi di comunicazione (gli *Internet Service Providers*) di adottare le opportune procedure di filtraggio.
Secondo un'interpretazione rigorosa dell'art.130 in esame, appare illecita anche un'unica e-mail non sollecitata avente scopo promozionale o pubblicitario, mentre non ha alcun pregio giuridico il *disclaimer* col quale il mittente si impegna a non spedire ulteriori comunicazioni e a cancellare gli indirizzi dei destinatari!
Risulta altresì irrilevante, la giustificazione che tali indirizzi non siano stati archiviati in un data

base (perché magari il titolare ha utilizzato un software che li genera con modalità *random*, cioè in maniera casuale).
Si ricorda, infine, che anche il decreto legislativo 9 aprile 2003 n.70 in materia di e-commerce si occupa di comunicazioni commerciali, ricomprendendo in questa definizione tutte quelle destinate, in modo diretto o indiretto, a promuovere beni, servizi oppure l'immagine di un'impresa, di un'organizzazione o di un soggetto che esercita un'attività agricola, commerciale, industriale, artigianale o una libera professione. In particolare, secondo tale decreto, le comunicazioni commerciali non sollecitate trasmesse via e-mail devono essere identificate come tali "in modo chiaro e inequivocabile" e fin dal momento della ricezione; anche in questo caso il destinatario dev'essere avvisato della facoltà di opporsi al ricevimento di successive comunicazioni.
È, inoltre, prevista un'importante presunzione a vantaggio del destinatario, in quanto la norma addossa al mittente l'onere di dimostrare che la comunicazione commerciale era stata sollecitata. Pertanto a carico di chi esercita un'attività di e-commerce sussistono i seguenti oneri (alcuni dettati anche dal Codice della privacy):
***a.*** ottenere il consenso da parte del consumatore all'invio di e-mail;
***b.*** rendere edotto il destinatario della possibile opposizione a futuri invii;
***c.*** non camuffare la propria identità nel messaggio;
***d.*** fornire un valido recapito al destinatario;
***e.*** avvisare, nell'oggetto dell'*e-mail*, che la medesima contiene una comunicazione commerciale.
Quest'ultima previsione si rivela molto utile per migliorare le procedure di filtraggio di cui si è accennato, soprattutto, quando viene utilizzata una sigla standard per indicare i messaggi pubblicitari (per esempio ADV) o gli annunci riservati agli adulti (ADLT), in maniera simile a quanto avviene nei gruppi di discussione per le e-mail off topic (contraddistinte dalle iniziali OT), [riquadro 1].

## La tutela penale e civile

Il destinatario di messaggi indesiderati che subisca un danno per effetto dello *spam* può ottenerne il risarcimento, sia della componente patrimoniale che non patrimoniale (per esempio il danno morale), eventualmente liquidabile in via equitativa qualora non ne risulti comprovato l'esatto ammontare.
Infatti, come ha riconosciuto il Giudice di Pace di Napoli, l'utilizzo della posta elettronica per l'invio di messaggi indesiderati comporta una lesione ingiustificata dei diritti dei destinatari, sotto due profili: da un lato per la scorrettezza e l'illiceità del trattamento dei dati personali dell'interessato e dall'altro lato per l'illegittima intrusione e invasione nella sua sfera di riservatezza. Nel caso in questione, una società è stata condannata al risarcimento nella misura di euro 1000 determinata equitativamente, sia per il danno materiale che per quello morale, tenuto conto delle spese generali e degli inconvenienti e perdite di tempo subite, derivante dall'illecito invio di corrispondenza elettronica a scopo pubblicitario non effettuato sulla base del consenso preventivo e informato, oltre alla rifusione delle spese processuali.
L'applicazione della normativa sulla protezione dei dati personali al fenomeno dello spamming comporta che l'utilizzo dell'indirizzo di posta elettronica (qualificabile a tutti gli effetti come trattamento di un dato personale) senza il rilascio dell'informativa possa essere punito con la sanzione amministrativa del pagamento di una somma da 3.000 a 18.000 €.
Inoltre la violazione delle regole stabilite dal D.lgs. 70/03 sopra richiamato, viene punita con il pagamento di una sanzione amministrativa pecuniaria da 103 a 10.000 €.
L'invio di *spam* può perfino configurare il reato di trattamento illecito di dati, fattispecie sanzionata con la reclusione da sei a diciotto mesi, purché si avverino entrambe le seguenti condizioni:
**1.** il fatto venga commesso al fine di trarne profitto (circostanza scontata nel caso di comunicazioni pubblicitarie, o comunque di natura commerciale, finalizzate per loro stessa logica e natura a un vantaggio economico e/o commerciale diretto o indiretto del soggetto che utilizza tale strumento di marketing);

**Riquadro 1**
**Le tre regole base del sistema italiano**
**1.** Le attività di marketing diretto per posta elettronica sono soggette al consenso preliminare degli abbonati (eccettuati i messaggi inviati da un'impresa ai propri clienti per proporre servizi o prodotti analoghi).
**2.** È illecito camuffare o mascherare l'identità del mittente a nome del quale viene effettuata la comunicazione.
**3.** Tutti i messaggi di posta elettronica devono contenere un indirizzo di risposta valido al quale l'abbonato può chiedere che non gli vengano più inviati messaggi.

**Riquadro 2**

**Responsabilità e sanzioni**

*Civili*: risarcimento del danno provocato al destinatario (sia materiale che morale).

*Amministrative*: sanzione pecuniaria da 3.000 a 18.000 € per l'omessa informativa; sanzione pecuniaria da 103 € a 10.000 € per la violazione del D.lgs. 70/03.

*Penali*: reclusione da 6 a 18 mesi per il trattamento illecito di dati personali (se dal fatto deriva nocumento).

**2.** ne sia derivato nocumento (secondo alcuni il danno nello *spam* è implicito, mentre altri richiedono un danno patrimoniale apprezzabile).
Solo il tempo e l'applicazione concreta di queste norme ne chiarirà l'effettiva portata, anche se ottime indicazioni possono essere ricavate dai provvedimenti emessi dal Garante negli ultimi anni, [riquadro 2].

## Le decisioni del Garante

L'Autorità garante per la protezione dei dati personali ha già avuto modo di intervenire in materia di comunicazioni indesiderate, anche prima dell'entrata in vigore del Codice della privacy, Dlgs 196/03, nonostante la legge 675/96 non contemplasse specificamente tale fattispecie.
Il provvedimento più significativo è senza dubbio il parere del 29 maggio 2003 che, sulla scorta dell'esperienza maturata nell'affrontare i ricorsi degli interessati, detta le regole fondamentali alle quali deve attenersi il titolare per un corretto invio delle *e-mail* pubblicitarie.
In primo luogo, secondo il Garante, la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet "*non legittima il titolare del trattamento ad inviare messaggi promozionali in assenza del preventivo consenso dell'interessato*".
Il consenso è necessario anche quando gli indirizzi vengono formati e utilizzati automaticamente, ovvero "*generati secondo procedure random, da uno speciale software sviluppato per questo preciso scopo*", anche in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e pure quando gli indirizzi non siano registrati dopo l'invio dei messaggi.
In particolare, i dati dei singoli utenti che prendono parte a *newsgroup* oppure a forum in Internet, sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per scopi diversi qualora manchi un consenso specifico.
Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista anagrafica degli abbonati a un *Internet provider* (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure pubblicati su siti web di soggetti pubblici per fini istituzionali laddove è comunque necessario "*avere riguardo alle specifiche finalità cui è preordinata la pubblicità dell'indirizzo elettronico*" (nel caso di specie si trattava dell'e-mail di un docente universitario).
Tali considerazioni valgono anche con riferimento ai messaggi pubblicitari inviati a gestori di siti web - anche di soggetti privati- utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio.
Per completezza si ricorda che i casi trattati dall'Autorità Garante non hanno riguardato e sanzionato solo imprese o società private che commercializzavano i propri prodotti o servizi, ma anche partiti politici e associazioni, accusate d'utilizzare la posta elettronica per propaganda elettorale.
I principi espressi nei provvedimenti menzionati conservano il loro valore anche con la vigenza del codice in materia di privacy, che oltre a riprendere i contenuti fondamentali della legge 675/1996, fornisce l'efficace strumento dell'art.130, sul quale potranno fare leva le nuove decisioni in tema di *spam* da parte del Garante e dei tribunali.

Antonio Piva laureato in Scienze dell'Informazione, Presidente, per il Friuli - Venezia Giulia, dell'ALSI (*Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica*) e direttore responsabile della Rivista di Informatica Giuridica.
Docente a contratto di Informatica giuridica all'Università di Udine.
Consulente sistemi informatici, valutatore di sistemi di qualità ISO9000 e ispettore AICA per ECDL base e advanced.
antonio_piva@libero.it

David D'Agostini avvocato, ha conseguito il master in informatica giuridica e diritto delle nuove tecnologie, fornisce consulenza e assistenza giudiziale e stragiudiziale in materia di *software, privacy* e sicurezza, contratti informatici, *e-commerce*, nomi a dominio, computer crime, firma digitale. Ha rapporti di partnership con società del settore ITC nel Triveneto.
Collabora all'attività di ricerca scientifica dell'Università di Udine e di associazioni culturali.
david.dagostini@adriacom.it