Brevi note in tema di tutela del consumatore nei contratti *on-line*. La responsabilità da *spamming*

di Carmine Galloro(1)

Sommario: 1) generalitá; 2) lo spamming alla luce della direttiva sul trattamento dei dati personali nel settore delle comunicazioni elettroniche; 3) la tutela dei consumatori nei contratti a distanza; 4) la tutela della privacy; 5) il controllo del garante; 6) profili civilistici della responsabilità da spamming.

1) Generalitá

Spamming è una parola di derivazione anglo-sassone che descrive un fenomeno molto noto a tutti coloro che utilizzano la posta elettronica: l'invio di materiale pubblicitario non richiesto e, spesso, non desiderato.

Negli Stati Uniti il fenomeno viene definito anche come *junk e-mail* e *bulk e-mail* . La sigla UCE (*unsolicited commercial e-mail*) sta a significare il messaggio di posta elettronica commerciale non richiesto, così come convenzionalmente indicato anche nei provvedimenti legislativi o regolamentari.(2)

Tale pratica oggi è assai diffusa nel mondo del cd. " *direct marketing* ", cioè quel campo di vendite in cui si applica in forma aggressiva il commercio diretto verso l'utente, mediante l'utilizzo di alcuni *software* in grado di copiare ed immagazzinare migliaia di indirizzi presenti sul *web* prelevandoli da siti, *forum* , *newsgroup* e, quindi, di spedire messaggi in pochi secondi a milioni di destinatari.

Tutto ciò, di contro, si riverbera in danno dei destinatari medesimi. Il soggetto titolare della casella di posta elettronica, ad esempio, è di fatto obbligato suo malgrado a rimanere connesso alla rete per scaricare o eliminare i messaggi *spamming* ed affrontare, nella maggior parte dei casi, i costi della connessione calcolati solitamente a tempo.

Senza contare che anche gli ISP (*internet service provider*), cioè i soggetti che materialmente forniscono l'accesso alla rete, sono allo stesso modo esposti al rischio di *crash down* , allorché risultino talmente intasati da materiali non sollecitati da non essere più in grado di recepire altri messaggi. Il che rappresenta un danno sia alla comunicazione tramite la rete che all'immagine commerciale del *provider* e dei vari siti di posta elettronica, poiché ciò genera inevitabilmente la diffidenza da parte degli utenti.

Sulla legittimità dell'invio di tali messaggi a fini informativi o pubblicitari, prima della regolamentazione prevista dalla direttiva 58/2002/CE (recepita in Italia nel testo unico sulla *privacy* , D. Lgs. n. 196/2003), si riteneva con eccesso di liberalità che le informazioni presenti sul *web* dovessero essere accessibili a tutti, fino a quando ciò rimaneva contenuto nell'àmbito del lecito.

Per cui non era da ammettersi il cd. " *spamming* industriale", e cioè l'attività consistente nell'invio indiscriminato, costante e ripetuto di milioni di messaggi attraverso diversi indirizzi di posta elettronica, volto ad intasare servizi *on-line* , senza il consenso del soggetto destinatario del messaggio pubblicitario. Oggi tale consenso – secondo la norma comunitaria – va richiesto dall'operatore preventivamente, una volta che questi abbia fornito la adeguata informazione sulle modalità e sulle finalità del trattamento.

È questo il sistema detto dell' *opt-in* , secondo il quale occorre che l'interessato significhi espressamente ed univocamente la propria accettazione prima d'essere inserito all'interno di un'operazione di trattamento. L'acquisizione del consenso e la conservazione documentale dell'avvenuta informativa, a loro volta, avranno valore probatorio in caso di contenzioso.

Negli USA, al contrario, è possibile trattare i dati personali degli interessati, qualora questi ultimi non avessero manifestato un loro esplicito dissenso, secondo il principio dell' *opt-out* . Vale a dire, il consenso si presume pienamente autorizzato sino al momento in cui viene manifestata l'opzione negativa.

Ed invero, in America sono state create delle liste (*black lists* o anche *Robinson's lists*) dove chiunque può iscriversi al fine di rendere noto a tutti gli operatori commerciali la propria indisponibilità a vedersi oggetto di trattamento. Di talché lo *sponsor* - prima di attingere alla banca-dati

contenente le informazioni sui destinatari - è tenuto a controllare all'interno delle *black list* i dati relativi alle *e-mail* di coloro che abbiano già preventivamente manifestato il loro dissenso.(3)

2) Lo *spamming* alla luce della direttiva sul trattamento dei dati personali nel settore delle comunicazioni elettroniche.

L'attività descritta può dirsi, in generale, illecita ogni volta che vìoli le norme di cui il combinato della direttiva comunitaria 2002/58/CE (4), recepita nel nostro ordinamento con il D. Lgs. n. 196/2003, detto anche "Codice della *Privacy* ". In particolare, si tratta delll' art. 13 della direttiva e l'art. 130 del Codice, entrambi rubricati "comunicazioni indesiderate"(5).

Come accennato sopra, la direttiva comunitaria in parola tende in sostanza a scoraggiare la commercializzazione diretta di beni o servizi effettuata tramite le moderne tecnologie di comunicazione (*fax* , *e-mail* , chiamate telefoniche automatiche) senza il preventivo consenso del destinatario(6).

Tuttavia, al secondo comma dell'art. 13 della citata direttiva si prevede la possibilità di inviare *e-mail* pubblicitarie anche a prescindere dal consenso espresso del destinatario dell'invio, purché(7)

a) il mittente sia un soggetto che svolga un'attività economica;

b) i soggetti destinatari delle comunicazioni commerciali siano suoi clienti;

c) lo *spammer* abbia ottenuto dai propri clienti gli estremi di posta elettronica nell'ambito di vendita di un prodotto o di fornitura di un servizio;

d) i servizi o i prodotti da commercializzare siano analoghi rispetto a quelli oggetto della vendita o del servizio, tramite i quali le coordinate elettroniche del cliente siano state raccolte.

Ma anche in tali casi, si prescrive che il cliente debba essere sempre informato circa l'utilizzo dei dati per finalità di commercializzazione diretta, in maniera chiara e distinta e salva sempre la possibilità di opporsi a tale uso.

Ad ulteriore tutela del diritto soggettivo del destinatario, al terzo comma dell'art. 13 in esame, si pone la facoltà per gli stati membri di adottare, in piena autonomia, tutti gli strumenti appropriati al fine di garantire l'effettività dell'opposizione all'invio di comunicazioni pubblicitarie, anche al di fuori dei casi previsti dai primi due commi dell'art. 13 medesimo.

Si nota in proposito che la norma stabilisce, da un lato, la gratuità dei rimedi a favore dell'interessato per l'esperimento delle misure contrastanti l'invasione della *privacy* , salve le spese relative ai costi di trasmissione del rifiuto (considerando n. 41). In pari tempo, occorre sottolineare che la stessa disposizione comunitaria devolve alle singole autorità statali la valutazione riguardo l' *opt-in* o l' *opt-out* , nei casi di *spamming* effettuato per finalità commerciali diverse dalla vendita di prodotti e dalla fornitura di servizi. Vale a dire, gli stati membri potranno decidere - a differenza di quanto avviene nel sistema USA - se l'illiceità dello *spamming* sia da ricollegare all'assenza di preventivo consenso dell'interessato abbonato, ovvero al suo espresso desiderio di non ricevere ulteriormente tale tipo di comunicazioni.

Emergono, tuttavia, alcuni dubbi sui limiti soggettivi di applicazione della disposizione in parola, considerando nella specie che il preventivo dissenso espresso dall'interessato è ammesso soltanto nei casi non previsti ai commi 1 e 2, cioè al di fuori dei casi di fornitura di servizi e di vendita di beni nei confronti di persone fisiche.

Dal che si evince una tutela maggiore in favore dei destinatari che siano persone giuridiche ed abbonati a tali prestazioni, delineandosi pertanto in tale ambito il profilo della disparità di trattamento nei confronti degli altri soggetti.

3) La tutela dei consumatori nei contratti a distanza

La disciplina comunitaria a tutela dei consumatori nei contratti a distanza, di cui la direttiva 97/7/CE, è stata introdotta nel nostro ordinamento con il D. Lgs. 22 maggio 1999, n. 185.

All'art. 1 di tale ultima disposizione è, appunto, specificata la nozione di contratto a distanza, quale " *contratto avente ad oggetto beni o servizi stipulato tra un fornitore e un consumatore nell'àmbito di un sistema di vendita o di prestazione di servizi a distanza organizzato dal fornitore che, per tale contratto, impiega esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto stesso* ".

Il regolamento contrattuale in questione, invero, deve essere corredato da tutte le informazioni richieste dall'utente di media diligenza, da esplicitarsi attraverso il sito *web* del fornitore. In genere, accade che la proposta e le relative condizioni vengano elencate pagina per pagina nelle finestre di dialogo che si succedono sullo schermo del *computer* , fino alla comparsa della casella riservata all'accettazione, collocata "in calce" al contratto. Al fornitore spetterà, poi, comunicare la conferma dell'avvenuto accordo, da inoltrarsi per iscritto o anche per posta elettronica.
A tutela dell'optante, la legge stabilisce il termine di dieci giorni ai fini dell'esercizio del diritto di recesso, tranne il caso in cui la stipula non sia avvenuta conformemente alla disciplina del contratto a distanza. In tal caso, il periodo è portato a tre mesi.
La scelta del legislatore a salvaguardia del consumatore nei contratti *on-line* è, infatti, operata in maniera da bilanciare la posizione di preminenza del fornitore, quale soggetto che impone attraverso clausole *standard* le modalità della prestazione e quant'altro ancora. In analogia a quanto avviene nel regime dei contratti conclusi al di fuori dei locali in cui si esercita il commercio, di cui il D. Lgs. n. 50/1992, attuativo della Direttiva CEE 85/577, esistono delle particolari cautele a cui i contraenti debbono conformarsi ai fini della regolarità dell'accordo. All'uopo, si rammenta che, in caso di confliggenza tra i sistemi contrattuali delineati, è stabilito all'art. 15 del D. Lgs. N. 185/99 l'applicazione delle disposizioni in ogni caso più favorevoli per il consumatore(8).
Per quanto inerisce l'utilizzo dello *spamming* da parte degli imprenditori, la norma prevista all'art. 10, in particolare, è intitolata " *limiti all'impiego di talune tecniche di comunicazione a distanza* " ed individua ulteriori limiti all'invio di materiale pubblicitario tramite l'introduzione di un duplice sistema autorizzatorio (commi 1 e 2)(9).
Ricalcando pedissequamente la già descritta disciplina posta a tutela della *privacy* , la norma predetta ha inteso fornire una maggiore e più incisiva tutela al destinatario di comunicazioni commerciali mediante *e-mail* , che si basa essenzialmente
sull'informazione riguardante il trattamento dei dati personali;
- sul consenso espresso a tale trattamento;
- sul diritto di opposizione al trattamento.

Nello specifico, al comma 1 dell'art. 10 del citato decreto opera l'esplicito divieto per il fornitore (ovvero la persona fisica o giuridica che nei contratti a distanza agisce nel quadro della sua attività professionale) di utilizzare telefono, posta elettronica ed altri sistemi automatici di chiamata senza il preventivo consenso dell'interessato.
Mentre il secondo comma dispone la facoltà di adoperare tecniche di comunicazioni a distanza diverse da quelle previste nel comma 1, laddove consentano una corrispondenza individuale e fin tanto che il consumatore non si sia dichiarato esplicitamente contrario.
Il regime in esame tende formalmente a tutelare i diritti soggettivi del consumatore che accede al *web* , approntando nei confronti di costui una serie di rimedi contro le insidie rappresentate dagli altri contraenti in malafede. Sicché, l'invio di corrispondenza che presenta contenuto e modalità dello *spamming* costituisce senza dubbio sia la violazione specifica della disciplina sulla *privacy* , così come della norma a tutela dei consumatori nei contratti conclusi a distanza(10).

4) La tutela della privacy

Contrariamente a quanto stabilito dalla direttiva europea sul trattamento dei dati personali, la norma italiana di recepimento ha notevolmente ampliato la tutela a favore del destinatario contro gli attacchi alla *privacy* (11).
Ed infatti, il legislatore comunitario si era limitato a prevedere l'obbligo del preventivo consenso del destinatario per l'invio di comunicazioni elettroniche solamente nei casi ascrivibili alla commercializzazione diretta di beni o servizi.
Nel nostro ordinamento, di contro, le modalità di sfruttamento di tali mezzi hanno trovato una più puntuale definizione, richiedendosi il consenso del destinatario nelle ipotesi di
- vendita diretta;
- invio di materiale pubblicitario;
- compimento di ricerche di mercato;
- compimento di comunicazioni commerciali.

Fuori da questi casi l'invio di comunicazioni non richieste può avere legittimamente luogo unicamente nel rispetto della disciplina prevista dagli artt. 23 e 24 del T. U. n. 196/2003, ovvero qualora sia stato richiesto il preventivo consenso dell'interessato all'utilizzo dei proprio dati personali (art. 23), oppure nei casi in cui il trattamento può svolgersi anche senza il consenso dell'interessato (art. 24, in relazione ai dati reperiti presso elenchi pubblici o registrati, sottoposti ad un regime di conoscibilità generalizzata come elenchi telefonici o registri elettorali).
Sotto tale profilo, va tuttavia notato che all'art. 130, come anche al comma 2 dell'art. 13 della direttiva 2002/58/CE, sia ritenuta ammissibile - anche senza il consenso dell'interessato - l'utilizzazione delle coordinate di posta elettronica fornite nell'àmbito della vendita di un prodotto o di un servizio.
Ma anche in tali casi, il limite alla liceità dello *spamming* è rappresentato dall'obbligo di informazione nei confronti del destinatario, riguardo la possibilità di poter ricevere in futuro messaggi reclamizzanti servizi o prodotti analoghi a quelli oggetto del precedente rapporto. Salva comunque la facoltà dell'interessato ad opporsi preventivamente o successivamente a tale invio.
Un'altra evidente analogia, rispetto alle previsioni della direttiva europea, la si coglie nel divieto di comunicazioni promozionali o di natura commerciale di cui l'art. 130 in questione, qualora il mittente sia camuffato o qualora questi celi la propria identità omettendo di fornire un idoneo recapito all'interessato.

5) il controllo del garante

Il Garante per la protezione dei dati personali ha sempre manifestato un orientamento restrittivo nei confronti dello *spamming* , anche prima dell'approvazione della direttiva 2002/58/CE e dell'entrata in vigore del T. U. sulla *privacy* . Al riguardo, si suole rammentare il contenuto di tre decisioni emesse dalla *Authority* negli ultimi anni, divenute oramai veri e propri punti di riferimento nella regolamentazione del fenomeno in parola: rispettivamente, quella del 11 gennaio 2001; del 13-19 maggio 2002; del 24-30 giugno 2002(12).
La prima pronuncia riguarda un ricorso avviato da alcuni destinatari di comunicazioni non desiderate di tipo politico, inviate tramite *e-mail* . Il *thema decidendum* ineriva la questione se una informazione di carattere personale, quale l'indirizzo di posta elettronica, dovesse essere o no considerata inserita in pubblico elenco e, quindi, soggetta a trattamento.
Ricalcando il parere 1/2000 dell'organo europeo di vigilanza nella materia (cd. “Gruppo Europeo”), l'Autorità italiana ha ritenuto illegittimo in base a tre ordini di motivi l'invio di propaganda politica nelle modalità citate; vale a dire:
il trattamento dei dati personali non deve avvenire in misura sleale;
è da definirsi “sleale” il trattamento dei dati per finalità diverse a quelle cui il destinatario aveva acconsentito;
il pregiudizio arrecato dalle spedizioni non autorizzate vìola il principio di proporzionalità tra gli interessi dello *sponsor* e quelli del destinatario.
Dal punto di vista ermeneutico, è importante rammentare che la disposizione di cui l'art. 12 della legge n. 675/96 disciplinava i casi in cui era possibile procedere ad un trattamento di dati in assenza del consenso dell'interessato, laddove si trattasse di dati provenienti da elenchi pubblici o registri accessibili da chiunque, a cui si ricollegavano alcune ulteriori tipologie e/o modalità individuate altrove dal legislatore. Quindi, non era sufficiente la piena conoscibilità di un dato per renderlo liberamente trattabile, bensì era necessaria l'esistenza di un regime giuridico di piena conoscibilità di quel dato da parte di chiunque.
Per assicurare una tutela piena ed efficace, il Garante ha stabilito pertanto i confini in cui potesse aversi l'accesso ai dati dei destinatari. In particolare, si è precisato che gli indirizzi *e-mail* presenti in *internet* non fossero assimilabili ai dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, e quindi non potessero essere trattati anche in assenza del consenso dell'interessato.
Tale orientamento va per vero collegato a quello già espresso con la *newsletter* n. 14/18.7.99 e con il comunicato dal 12 luglio 1999, laddove la stessa Autorità ebbe modo di affermare che “ *i messaggi che circolano via e-mail e nelle newsgroup sono da considerare corrispondenza e come tali non possono venire violati* ”(13).
La seconda pronuncia è del 2002 e concerne, in particolare, il fenomeno

dello *spamming* effettuato da una società fornitrice di servizi di *hosting* per un dato sito *web* .
Tale società era già stata direttamente intimata – ai sensi dell'art. 13 L . 675/96 – affinché cessasse l'attività contestata e dichiarasse all'interessato
- l'origine dei dati personali che lo riguardavano;
- il responsabile del trattamento dei dati medesimi;
- la prova della eventuale autorizzazione al trattamento;
- la prova dell'eventuale consenso al trattamento in favore di terzi.

In sede di contenzioso, l'Autorità accoglieva sostanzialmente le doglianze del ricorrente in relazione alle questioni predette, ribadendo il principio del consenso preventivo siccome " *è illegittimo utilizzare a scopi commerciali un indirizzo e-mail, che non compare in elenchi pubblici, senza il consenso del destinatario* ".
Quanto alla conseguente domanda risarcitoria, veniva liquidata la somma forfettaria di duecentocinquanta euro per la sorta relativa alle spese del procedimento, essendo stata devoluta al Magistrato ordinario la questione inerente la riparazione dei danni.
In pari tempo, veniva correttamente attivata d'ufficio la autonoma procedura per l'applicazione delle eventuali sanzioni, ai sensi del primo comma dell'art. 31, *lett* . b, della L. 675/96.
Ancora nel 2002 veniva adottata la terza delle decisioni sopra citate, a séguito del ricorso di un docente universitario contro l'invio di posta elettronica non autorizzata, verso l'indirizzo *e-mail* riportato nel sito della stessa Università.
Anche in questo caso il Garante stabiliva che " *la presenza dell' indirizzo e-mail di una persona su un sito internet non autorizza le aziende, per il solo fatto di essere pubblico, ad utilizzarlo per inviare pubblicità* " e quindi " *i dati posti a disposizione del pubblico per circoscritte finalità, ad es. di tipo istituzionale come nel caso in esame, non sono, infatti, liberamente utilizzabili per l'invio generalizzato di e-mail. E questo anche quando le e-mail non abbiano un contenuto commerciale o pubblicitario. Per poter procedere all'invio dell'e-mail all'indirizzo di posta elettronica del docente, la società avrebbe dovuto, dunque, ottenere prima il suo consenso. Non avendo né richiesto né ottenuto tale consenso la società ha, pertanto, violato le norme sulla privacy. Di conseguenza, la società non poteva limitarsi ad inserire il nominativo del ricorrente in una lista di soggetti non interessati all'invio di messaggi pubblicitari, ma aveva l'obbligo di cancellare i dati del ricorrente ed astenersi in futuro dall'utilizzare quei dati per scopi commerciali l'indirizzo e-mail presso l'Università* ".
Con riferimento specifico allo *spamming* tramite telefonate commerciali, meritano d'essere rammentate alcune pronunce che – se correttamente applicate – eliminerebbero o almeno limiterebbero l'invadenza di certi fenomeni.
In primo luogo, l'Autorità ha affermato con parere pubblicato nella *newsletter* del 6-12 novembre del 2000(14) che " *se un cittadino non vuole ricevere telefonate commerciali, le società che lo hanno contattato, anche in base a dati ottenuti ed utilizzati correttamente, devono cancellare senza ritardo i dati in loro possesso, fornendo anche una attestazione che la cancellazione è avvenuta ed è stata resa nota anche ad eventuali altre società alle quali i dati erano stati precedentemente comunicati* ".
Successivamente, lo stesso Garante ha avuto modo di esprimere tale orientamento circa l'utilizzo di *spamming sms* , ritenendo scorretto l'invio sul telefonino dell'utente di messaggi promozionali, relativi a servizi offerti dal gestore di telefonia mobile, senza l'espresso consenso a ricevere questo tipo di informazioni(15). Parimenti è da ritenersi illecito l'espediente, adottato da alcuni fornitori di servizi telefonici, di subordinare la stipula del contratto o l'attivazione della carta prepagata alla prestazione del consenso a ricevere messaggi pubblicitari, o quello di dissimulare comunicazioni commerciali dietro fittizie informazioni di servizio alla propria utenza(16)
Tale giurisprudenza è stata poi ribadita nel Comunicato del 3 settembre del 2003 e nella *newsletter* 1-7 settembre 2003, laddove si precisa che " *inviare e-mail pubblicitarie senza il consenso del destinatario è vietato dalla legge. Se questa attività, specie se sistematica, è effettuata a fini di profitto e vìola anche una norma penale, il fatto può essere*

denunciato all'autorità giudiziaria "(17).
Per quanto concerne il delicato tema della pubblicità elettorale, si rammenta il Provvedimento Generale del Garante del 7 settembre 2005 (cd. "decalogo"), in cui vengono fissate le regole generali sulle informazioni utilizzabili dai candidati e con quali modalità(18).
Tra i dati trattabili senza consenso rientrano quelli contenuti nelle liste elettorali dei Comuni, da utilizzarsi per contattare gli elettori ed inviare materiale di propaganda da parte di organismi politici, comitati promotori, sostenitori e singoli candidati.
Possono essere usati liberamente anche altri elenchi e registri in materia, come l'elenco degli elettori italiani residenti all'estero ed iscritti all'AIRE, oltre ad altre fonti documentali accessibili a chiunque (es. albi professionali). Sono trattabili altresì i dati degli abbonati presenti nei nuovi elenchi telefonici, accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere posta o telefonate.
Non sono invece accessibili a tale scopo - neanche da parte di titolari di cariche elettive - gli archivi dello stato civile, l'anagrafe dei residenti, gli indirizzi raccolti per svolgere attività e compiti istituzionali o per prestazioni di servizi, anche di cura.
Nei casi in cui è necessario il previo consenso - a meno che i dati personali siano stati forniti direttamente dall'interessato – sono ricomprese quelle particolari modalità di comunicazione elettronica come *sms* , *e-mail* , *mms* , telefonate preregistrate e *fax* . Così come si ritiene necessario il regime di *opt-in* ai fini della raccolta automatica dei dati su *internet* o ricavati da *forum* o *newsgroup* , dalle liste di abbonati ad un *provider* e, in genere, dalle informazioni presenti sul *web* per altre finalità.

6) Profili civilistici della responsabilità da *spamming*
In àmbito europeo, la giurisprudenza ha cominciato a considerare solo da poco tempo il fenomeno in parola, censurando la condotta dell'autore e mittente dei messaggi non sollecitati ai fini del risarcimento del danno.
Si segnala in merito la vicenda trattata dai giudici francesi(19) e riguardante non i diritti soggettivi dei destinatari, bensì quelli invocati da due fornitori di servizi elettronici in rete. I quali non potevano pertanto lamentare la violazione delle norme in materia di *privacy* e di riservatezza individuale, dovendo limitare la pretesa risarcitoria al solo danno di immagine causato alla loro attività da parte dell'utente sleale.
Nella specie, lo *spammer* esercitava un'attività d'impresa inerente la vendita a distanza, sostenendo all'uopo una ossessiva campagna di informazione commerciale rivolta al pubblico tramite *e-mail* . Tale corrispondenza avveniva utilizzando il servizio di posta elettronica di un certo *provider* al quale costui era abbonato, ed era indirizzata ai destinatari utenti di un certo altro servizio di messaggeria.
A sèguito di numerose denunce da parte dei clienti che lamentavano la ricezione dei messaggi non sollecitati, il fornitore del servizio di messaggeria faceva ricorso al Tribunale di Nanterre, attraverso istanza al Presidente, richiedendo all'altro *provider* l'esibizione della documentazione riguardante l'imprenditore mittente.
Eseguendo l'ordinanza emessa dal Giudice adìto, il *provider* medesimo comunicava le informazioni a sua disposizione per identificare l'autore dell'attività denunciata, promuovendo, quindi, un autonomo giudizio contro costui per inadempimento delle condizioni contrattuali poste all'utilizzo del servizio *e-mail* . Le due cause venivano riunite dal Tribunale di commercio di Parigi, davanti al quale il resistente articolava la difesa sostanzialmente in quattro punti:
- avendo cessato il suo sito ogni attività, le *e-mail* inviate successivamente erano da attribuirsi a persone che potevano utilizzare la risorsa elettronica messa a disposizione dal *provider* a sua insaputa;
- il contratto con il *provider* stesso era da considerarsi "virtuale", in quanto non prevedeva sottoscrizione;
- le condizioni di utilizzazione dei servizi *on-line* erano riportate in maniera prolissa e poco intelligibile, poiché redatte appositamente in modo da impedire la lettura dell'intero documento;
- in ogni caso, era consentito al destinatario del messaggio pubblicitario di bloccare l'invio di altre *e-mail* allo stesso indirizzo.

All'esito del dibattimento, il Collegio accertava, alla stregua delle circostanze di fatto, la validità dei contratti in contestazione. E pertanto dichiarava la sussistenza dell'attività di *spamming* , svolta attraverso

l'utilizzo rispettivo dei servizi di posta e di messaggeria elettronica.
Tuttavia, in mancanza di elementi che consentissero di valutare il pregiudizio ai fini della quantificazione del danno materiale, il Tribunale francese condannava il convenuto a risarcire esclusivamente il danno causato all'immagine dei servizi predetti, peraltro quantificato in via equitativa.
Riguardo la giurisprudenza italiana in materia, si citano usualmente due sentenze del Giudice di Pace di Napoli, rispettivamente del 7 e del 26 giugno 2004(20), le quali hanno per oggetto la richiesta di risarcimento danni avanzata dai destinatari, a causa della lesione della propria sfera di riservatezza e della propria *privacy* causata dall'invio indesiderato e non sollecitato di messaggi *e-mail* ovvero di *sms* .
Entrambe le sentenze giungono a condannare i convenuti al risarcimento del danno, attraverso un percorso logico – giuridico abbastanza tradizionale, poiché ricollegano la responsabilità civile connessa all'attività di *spamming* nell'àmbito della responsabilità extracontrattuale (art. 2043 c.c.), anziché nell'ambito della responsabilità connessa allo svolgimento di attività pericolose (art. 2050 c.c.). La differenza fra queste due impostazioni ha riverberi sia sul piano sostanziale che processuale.
Se si riconduce la responsabilità civile nella responsabilità extracontrattuale, l'onere probatorio ricade sul danneggiato, il quale deve dimostrare i danni subiti oltre al dolo o alla colpa del soggetto agente, nonché il nesso di causalità fra l'azione e l'evento dannoso.
Nel caso in cui l'attore invochi, al contrario, il risarcimento ai sensi dell'art. 2050 c.c., è previsto l'onere di dimostrare i danni subiti, oltre al nesso di causalità, ad esclusione della prova dell'elemento psicologico dell'illecito (dolo o colpa). Per cui incombe sulla controparte l'onere di dimostrare di aver adottato tutte le misure idonee ad evitare il danno.
Nelle sentenze in esame, il Giudice ha riconosciuto la illiceità dell'attività di *spamming* ai sensi dell'art. 2043 del codice civile, condannando il responsabile a cancellare i dati del richiedente dai propri archivi elettronici, oltre a risarcire i danni non patrimoniali derivanti dall'ingiusto turbamento arrecato alla vita privata del destinatario del messaggio pubblicitario, liquidandoli secondo equità nella somma di mille euro più settecentocinquanta euro a titolo di spese legali.
Si evidenzia nello specifico che lo stesso Giudice napoletano ha riconosciuto la risarcibilità anche del danno non patrimoniale, rappresentato dal " *danno alla vita di relazione del danno esistenziale conseguente alla lesione e al turbamento della qualità di vita dell'attore* "; oltre a quello patrimoniale derivante dalle " *spese generali e gli inconvenienti e perdite di tempo subite* "(21).
In generale, si osserva che la pronuncia del 10 giugno evita di seguire il disposto normativo che appositamente disciplina il risarcimento per illecito trattamento dei dati personali, vale a dire l'art. 18 della L. 675/96, oggi art. 15 del D. Lgs.. 196/03, cd. T.U. della *privacy* , e, di conseguenza, la disposizione fondamentale sulla regolamentazione della colpa nelle attività pericolose, di cui l'art. 2050 c.c(22).
Ed infatti tale decisione privilegia – al pari della successiva – la ricostruzione della condotta illecita sul modello della colpa extracontrattuale, secondo la clausola generale prevista all'art. 2043 c.c. anche per i casi in cui non si abbia la violazione di norma specifica.
La scelta è di ordine sistematico ed appare giustificata dalla ragione che il collegamento, tra la disciplina espressamente prevista a tutela della *privacy* e la responsabilità di cui l'art. 2050 c.c., si dimostra per qualche verso sproporzionato. A fronte di una normativa (di derivazione comunitaria) puntuale e delineata caso per caso, fa infatti da contraltare la regola codicistica predisposta a tutt'altro scopo, laddove il soggetto agente è chiamato a rispondere a titolo di colpa presunta (anche di tenuissima entità)(23) ovvero a sèguito di responsabilità oggettiva(24).
Ed invero, attraverso tale norma si è inteso assicurare il massimo grado di protezione in relazione ai danni cagionati da attività pericolosa in generale, con ciò intendendo " *quelle attività previste all'art. 46 e ss. del T. U. delle leggi di pubblica sicurezza, oltre a quelle prese in considerazione per la prevenzione degli infortuni o la tutela dell'incolumità pubblica, e tutte le altre che, pur non specificate o disciplinate, abbiano tuttavia una pericolosità intrinseca o comunque dipendente dalle modalità di esercizio o dai mezzi di lavoro impiegati* ".(25)
Orbene, che il legislatore abbia voluto fornire una tutela pregnante ed incondizionata anche al principio della riservatezza è certamente

encomiabile, alla luce dell'erosione costante e crescente del diritto di ognuno " *to be alone* ". Ed appare condivisibile, pertanto, annoverare tra le attività pericolose sopra descritte la condotta rivolta ad attingere e divulgare i dati identificativi delle persone, atteso che si tratta pur sempre della lesione dei cd. diritti fondamentali, i quali sono sanciti al più alto livello nelle convenzioni e negli ordinamenti internazionali.
Con riguardo al fenomeno particolare dello *spamming* , si evidenzia in primo luogo la mancanza di una specifica fattispecie legislativa, per cui la descrizione dell'illecito in questione non può che operarsi attraverso una ricostruzione empirica diversa dal collegamento richiamato dalle norme sulla *privacy* . Alcuni dubbi sulla ragionevolezza di tale analogia sorgono, infatti, all'esame delle modalità di estrinsecazione della condotta sanzionata; consistente, appunto, nell'emissione ossessiva e sistematica di corrispondenza non desiderata a fini pubblicitari e/o commerciali. Di talché il "dolo specifico" è da rinvenirsi nello scopo ulteriore e successivo rappresentato dal vantaggio economico, a cui mira il soggetto agente.
Ad esempio, è risaputo che, in moltissimi casi, l'invio di *spam* e *pop up* avviene sulla scia dei *cookie* che l'utente lascia nella rete dopo aver visitato determinati siti *web* ; sicché agli imprenditori fraudolenti resta soltanto da calcolare statisticamente quante volte l'utente ha avuto accesso a taluni siti, al fine di risalire agli interessi ed alle inclinazioni di costui, non rilevando in alcun modo l'età, la professione o quant'altro. Dopodiché, è gioco facile spedire la messaggeria indesiderata (inerente automobili, viaggi, informatica, ecc.) in modo massiccio e pervasivo.(26)
In ogni caso il rischio connesso alla condotta dello *spammer* è, come già visto, quello di intasare la casella di posta elettronica del destinatario o, addirittura, quello di far collassare il sistema del *provider* .
Sembra, allora, una sorta di forzatura quella di includere lo *spamming* tra le attività intrinsecamente pericolose (cioè, accesso e trattamento dei dati identificativi delle persone) descritte dal combinato di cui gli artt. 15 del D.Lgs. 196/2003 e 2050 del codice civile , poiché la violazione del diritto alla riservatezza costituisce, nella specie, solo un fine indiretto e secondario.
Per quanto attiene il profilo strettamente risarcitorio, occorre evidenziare peraltro che uno strumento sicuramente più efficace si dimostra il rimedio di cui l'art. 2043 c.c. Ed infatti si può rammentare che il tipo di responsabilità, a cui fa richiamo la predetta norma sulle attività pericolose, prescinde da ogni indagine sull'elemento psicologico, stabilendo al riguardo una severissima presunzione di colpa, superabile solamente con l'esperimento della prova liberatoria.
Cosicché in base a tale disciplina perderebbe rilevanza il dato soggettivo, rappresentato dal dolo e dal grado di intenzionalità con cui l'evento dannoso è stato cagionato. Di conseguenza, rimarrebbe preclusa la valutazione del danno adeguatamente ancorata ai criteri indicati dall'ordinamento, a seconda della fattispecie dolosa o colposa.
È auspicabile, dunque, un intervento del legislatore o della giurisprudenza per dare contorni certi alla tipologia in questione, se non altro per evitare il rischio di svalutare la portata normativa dello stesso art. 2050 c.c. e, per l'effetto, dare la stura ad un'interpretazione inflazionistica dei princìpi in esso contenuti.
Occorre precisare, sotto altro aspetto, che le due sentenze esaminate facevano riferimento a controversie sorte nel 2003, ovvero prima dell'entrata in vigore del codice privacy, laddove si prevede, quale giudice competente per le controversie in tema di violazioni del codice sulla protezione dei dati personali, il tribunale in composizione monocratica.
Ai sensi dell'art. 152 del D. Lgs. 196/2003, inoltre, il foro territorialmente competente è da individuarsi in base alla residenza o al domicilio del ricorrente, posto che l'atto introduttivo del giudizio non è la più citazione bensì il ricorso.(27)

Note
(1) Dottorando di ricerca
(2) G. CASSANO, Internet e riservatezza , in Internet. Nuovi problemi e questioni controverse , a c. di G. Cassano, Milano, 2001, pag. 27; E. RUGGIERO , Il contratto telematico, Napoli, 2003, pag. 82; M. ATELLI, Spamming: si svolta verso il silenzio assenso, in Guida al Diritto, 2003, 20, pag. 45; G. BRIGANTI, Spamming e diritto, in www.iusreporter.it; L.

M. De Grazia, Spamming : definizioni ed aspetti legali , in “Diritto & Diritti”, www.diritto.it; C. ERCOLANO, Spamming: una nuova forma di pubblicità dannosa per i consumatori?, in Diritto della Gestione Digitale delle Informazioni, suppl. n. 9 Il Nuovo Diritto, 9, pag. 44 ss . ; A. LEVI, F. ZANICHELLI, L'utilizzo dell'E-Mail a fini pubblicitari: dallo "spamming" al "permission marketing"; in Riv. Dir. Ind., 2001, I, 194.

(3) E. RUGGIERO , Il contratto telematico, cit., Napoli, 2003, pag. 85; E. A. ALONGI, *Has the U.S. Canned Spam?* , in Arizona. L. Rev., 2004, 3, pag. 46; B. G. Gilpin, *Attorney Advertising & Solicitation on the Internet: Complying with Ethics Regulations and Netiquette* , in Journal Marshall J. Computer & Info, 11, 1995; D. E. SORKIN, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 , in Buffalo L. Rev., 1997, 10, pag. 45.*

(4) In particolare recita al riguardo il considerando n. 6 della direttiva: “'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata”. Al riguardo, stabilisce la prima parte del considerando n. 40: “Occorre prevedere misure per tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta, in particolare mediante dispositivi automatici di chiamata, telefax o posta elettronica, compresi i messaggi sms”.

(5) L'art. 13, della direttiva così dispone “ *1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso.*

2. Fatto salvo il paragrafo 1, allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, a condizione che ai clienti sia offerta in modo chiaro e distinto al momento della raccolta delle coordinate elettroniche e ad ogni messaggio la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora il cliente non abbia rifiutato inizialmente tale uso.

3. Gli Stati membri adottano le misure appropriate per garantire che, gratuitamente, le comunicazioni indesiderate a scopo di commercializzazione diretta, in casi diversi da quelli di cui ai paragrafi 1 e 2, non siano permesse se manca il consenso degli abbonati interessati oppure se gli abbonati esprimono il desiderio di non ricevere questo tipo di chiamate; la scelta tra queste due possibilità è effettuata dalla normativa nazionale.

4. In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni.

5. Le disposizioni di cui ai paragrafi 1 e 3 si applicano agli abbonati che siano persone fisiche. Gli Stati membri garantiscono inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente alle comunicazioni indesiderate”

(6) A proposito delle comunicazioni inviate a mezzo *telefax* , posta elettronica e dispositivi automatici di chiamata il considerando n. 41 della direttiva 2002/58/CE dispone *: “Tali forme di comunicazioni commerciali indesiderate possono da un lato essere relativamente facili ed economiche da inviare e dall'altro imporre un onere e/o un costo al destinatari. Inoltre, in alcuni casi il loro volume può causare difficoltà per le reti di comunicazione elettronica e le apparecchiature terminali. Per tali forme di comunicazioni indesiderate a scopo di commercializzazione diretta è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi”*.

(7) G. CASSANO, *Internet e riservatezza* , *cit* ., pag. 46 e ss.; E. RUGGIERO , Il contratto telematico, *cit* ., Napoli, 2003, pag. 95; G. BRIGANTI, *Spamming e diritto* , *cit* ., par. 2.2.

(8) Per una panoramica sul diritto continentale vigente in materia, si veda: A. PÜTZHOVEN, *Europäischer Verbraucherschutz im Fernabsatz. Die Richtlinie 1997/7/EG und ihre Einbindung in nationales Verbraucherrecht* , Monaco, 2001, pagg 72 e ss.; J. ALLIX, *La Directive 97/7/CE: Contrats conclus à distance et protection des consommateurs* , in Revue des Affaires europèennes, 1998, pagg. 176 e ss.; D. LANGER, *Verträge mit Privatkunden im Internet* , Colonia, 2003, pagg. 246 e ss; E. JAYME, C. KOHLER, *Europäisches Kolissionsrecht: Anerekennungsprinzip statt IPR?* , in Praxis des internationalen Privat- und Verfahrensrecht; 2001, pagg. 501-514; L. THÈVENOZ, *Le project de directive sur la comercialisation à distance des services financiers* , in H. STAUDER, B. STAUDER «La protection des consommateurs acheteurs à distance», Zurigo, 1999, pagg. 57-85.

(9) Così, l'art. 10 del D. Lgs. 185/99: " *1. L 'impiego da parte di un fornitore del telefono, della posta elettronica di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore;*

2. Tecniche di comunicazione a distanza diverse da quelle di cui al comma 1, qualora consentano una comunicazione individuale, possono essere impiegate dal fornitore se il consumatore non si dichiara esplicitamente contrario".

(10) C. MACRÌ, *Contratti negoziati fuori dai locali commerciali* , Torino, 1998, pag. 132; P. PERLINGIERI, *Metodo, categorie, sistema nel diritto del commercio elettronico* , in S. SICA, P. STANZIONE, " Commercio elettronico e categorie civilistiche", Milano, 2002, pagg. 10e ss.;. C: SCOGNAMIGLIO, *La conclusione e l'esecuzione del contratto telematico* , *ibidem* .

(11) G. CASSANO, *cit* ., pagg. 19 e ss.; F. DE MAGISTRIS, *La direttiva europea sul commercio elettronico* , in "Informatica giuridica", Napoli, 2001, pag. 169; A: MONTI, *Spam e indirizzi mail. Quando la 675 è impotente* , in www.interlex.it.

(12) www.garanteprivacy.it; E. RUGGIERO , Il contratto telematico, *cit* ., Napoli, 2003, pagg. 90 e ss.

(13) www.garanteprivacy.it.

(14) www.garanteprivacy.it.

(15) *newsletter* 3-9 febbraio 2003, in www.garanteprivacy.it.

(16) Parere del 10 giugno 2003, in www.garanteprivacy.it.

(17) www.garanteprivacy.it.

(18) In Gazzetta Ufficiale del 12.9.2005, n. 212 - Serie generale.

(19) Trib. Commercio Parigi, 5.5.2004, Foro It., 2004, 4, 510.

(20) Giudice di pace Napoli, sez. I, 10.6.2004, in Guida al Diritto, 2004, 32, 78; sez. I, 26.6.2004, in Foro It., 2004, 1, 2908.

(21) Così stabilito nella sent. --- " *L'invio di posta elettronica indesiderata nella fattispecie è illegittima sotto due profili: da un lato per la scorrettezza e illiceità del trattamento dei dati personali dell'attore da parte della convenuta e dall'altro lato provoca una illegittima intrusione e invasione nella sua sfera di riservatezza come stabilito dal Garante della privacy (gli indirizzi di posta elettronica non sono utilizzabili da chiunque in quanto non si tratta di dati pubblici alla stregua degli elenchi telefonici tradizionali)".*

(22) Questo il contenuto, rispettivamente, degli artt. 15 del D.Lgs. 196/2003 e 2050 del codice civile. Art. 15 (Danni cagionati per effetto del trattamento): " *1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 " ;* Art. 2050 *(Responsabilità per l'esercizio di attività pericolose)* : " *Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno* ".

(23) Cass. civ., sez. III, 24 febbraio 1983, n. 1425, in www.notiziariogiuridico.it; in dottrina, C .M. BIANCA, *Diritto civile, V* , Milano, 1994, pag. 709; L. ROVELLI, *La responsabilità civile da fatto illecito* , Torino, 1965, pag. 343.

(24) Cass. Civ., sez. III, 29 aprile 1991 , n. 4710 , in Mass. Foro It., 1991 , c. 397; in dottrina, M. COMPORTI, *Esposizione al pericolo e responsabilità civile* , Napoli, 1965, pag. 176; L. ENNECCERUS u. M. LEHMANN, *Recht der Schuldverhältnisse* , Tübingen, 1958, pag. 920; M. FRANZONI, *La responsabilità oggettiva. Il danno da cose e da animali* , Padova, 1988, pag. 462; P. TRIMARCHI, *Rischio e responsabilità oggettiva* , Milano, 1961, pag.11.

(26) Cass. Civ., sez. III, 20 luglio 1993 , n. 8069, in Foro it, 1994, I, 455.

(26) È questo il fenomeno noto con il nome di "profilazione", descritto normativamente all'art. 10 del D. Lgs. 185/99, attuativo della direttiva 97/7/CE.

(27) Q uesto il testo dei primi commi dell'art. 152 del D. Lgs. 196/2003 (Autorità giudiziaria ordinaria): *"1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.*

2. Per tutte le controversie di cui al comma 1 l 'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

3. Il tribunale decide in ogni caso in composizione monocratica.

4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.