Informatica e diritto, XXIX annata, Vol. XII, 2003, n. 1-2, pp. 172-196

Spam e tutela della riservatezza

EMANUELE FLORINDI*

SOMMARIO: *1. Che cos'è lo* spam *– 2. Una definizione di* spam *– 3.* E-mail *e pubblici elenchi – 4. I danni causati dallo* spam *– 5. I mezzi di difesa – 6. La normativa in materia – 7. Liceità delle* cd black list

1. CHE COS'È LO *SPAM*

Pur non trattandosi, almeno per il momento[1], di un reato in senso stretto

* L'Autore è consulente in diritto dell'informatica e responsabile del Centro studi e ricerche dell'associazione Telefono arcobaleno ONLUS.

[1] Sono state avanzate, in varie sedi, proposte relative all'introduzione del reato di *spam*, ma non è stata ancora formulata nessuna proposta precisa in merito. Si veda, però, l'articolo 130 del Decreto Legislativo, 30 giugno 2003, n.196, *Codice in materia di protezione dei dati personali*, pubblicato in GU n. 174 del 29-7-2003 - Suppl. Ord.n.123 - Testo in vigore dal 1-1-2004 in cui si prevede: «Art. 130 (Comunicazioni indesiderate)

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24.

4. Fatto salvo quanto previsto nel comma 1 , se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni».

lo *spam*[2] rappresenta oggi uno dei principali problemi di *internet*, nonché un ostacolo sempre maggiore alla libertà delle comunicazioni informatiche.

Nei primi mesi del 2003, infatti, l'intera comunità di *internet* si è trovata di nuovo a discutere in merito ad una questione che, pur datata, sembra avere di recente acquistato una vitalità tutta nuova rivelandosi in tutta la sua gravità.

Si tratta del cosiddetto *spamming* che, nato con il diffondersi della rete, dal 1994 affligge in maniera sempre più grave i *provider* ed i relativi utenti[3].

Per lungo tempo, lo *spamming* è stato assimilato alla distribuzione dei volantini pubblicitari nelle cassette per le lettere e, pertanto, ampiamente sottovalutato dal legislatore, ma, in realtà, questo fenomeno è molto diverso dal normale volantinaggio pubblicitario in quanto ha un costo per gli ignari destinatari.

Questi, infatti, per poter leggere la propria posta, ivi compresi i messaggi pubblicitari, sono costretti a collegarsi alla rete, e, quindi, a pagare, anche per leggere comunicazioni, indesiderate, indesiderabili e spessissimo prive di ogni utilità[4].

Per esemplificare possiamo paragonare lo *spamming* ad un volantinaggio in cui i volantini vengono inviati attraverso la posta ordinaria, con spese postali a carico del destinatario, senza che questi abbia alcuna pos-

[2] Nel gergo della rete, ma ormai anche nel linguaggio comune, con questo termine si indica l'invio, massiccio ed indiscriminato di messaggi di posta elettronica. Il nome nasce da una scenetta comparsa in un episodio di una popolare serie inglese; in cui una coppia entra in un ristorante, si siede ad un tavolo, ma quando arriva una cameriera per prendere le ordinazioni, dal tavolo vicino un gruppo di disturbatori inizia ad urlare «*Spam*, *spam*, *spam*…» in maniera così fragorosa che i due clienti non riescono neppure a capire quali pietanze siano in menù; d'altra parte anche la voce dei clienti è coperta dalle grida, pertanto questi si ritrovano costretti ad ordinare *spam* (SPiced hAM, marca di carne in scatola della Hormel). Per tale ragione, il termine *spam* è stato utilizzato per indicare un disturbo talmente grave da ostacolare la possibilità di comunicare ed infine, con il diffondersi di Internet, la posta spazzatura.

[3] Si veda, a tale proposito il commento di A.G. CAVALIERE, *Antispam: con Spews al bando il diritto alla e-mail!*, in vnunet.it, 14/01/2003, nonché G. LIVRAGHI, *La piaga dello spam*, in interlex.it, 12/09/02.

[4] Non può poi omettersi di considerare che vi sono degli abbonamenti ad internet in cui l'utente paga non in base al tempo di collegamento, ma sulla base del traffico generato e, quindi, anche in base alle e-mail ricevute. In tali situazioni la spesa dell'utente a causa dei messaggi di *spam* è ancora più evidente.

sibilità di rifiutarsi di riceverli: è necessario pagare e poi, eventualmente, gettare i volantini sgraditi.

Gli utenti subiscono, inoltre, un costo indiretto a causa dello *spamming* dato che i *provider* incorrono in costi aggiuntivi, per essere in grado di ricevere e smistare un volume sempre crescente di questo tipo di posta non desiderata.

Detti costi, imputabili all'utilizzo di banda, tempo dei processori, spazio su supporti di memorizzazione, in qualche maniera, dovranno poi essere caricati sugli utenti finali del servizio[5].

[5] A titolo di esempio, AOL stima in circa 2$ al mese il costo aggiuntivo per utente imputabile direttamente allo spam. In relazione all'altissimo costo sociale dello spamming è doveroso osservare che la Commissione europea (Direzione Generale XV del Mercato Interno) ha recentemente deciso di affidare ad una società di consulenza (ARETE) la conduzione di uno studio relativo al fenomeno dei messaggi di posta elettronica contenenti comunicazioni commerciali indesiderate. I risultati di detta analisi sono stati pubblicati alla fine del mese di gennaio 2001 in due parti distinte: la prima analizza l'attuale «stato dell'arte» per quanto concerne le tecnologie alla base dello spamming (con particolare riferimento alla situazione esistente negli USA), la seconda rappresenta un'analisi delle strategie normative adottate in Europa; seguono poi alcune considerazioni conclusive e di indirizzo al fine di promuovere lo sviluppo del commercio elettronico in Europa tutelando i diritti riconosciuti agli internauti europei. In particolare la Commissione ha osservato che, se veramente gli operatori avranno presto a disposizione sistemi che consentono di inviare 100 milioni di e-mail commerciali al giorno, e supponendo che siano 200 le imprese in grado di dotarsi di questi strumenti, i 300 milioni di utenti Internet potranno ricevere mediamente oltre 60 e-mail pubblicitarie al giorno. È stato stimato che ciò comporterebbe un costo medio di connessione per utente di oltre 30 euro/anno e su scala mondiale, nell'ipotesi che entro breve la comunità online raggiunga i 400 milioni di persone, i costi complessivi legati allo scaricamento di messaggi pubblicitari con le attuali tecnologie si possono valutare, per difetto, nell'ordine dei 10 miliardi di euro (e stiamo parlando solo dei costi sostenuti da chi naviga su Internet). Fonte: NEWSLETTER del Garante per la protezione dei dati personali del 12 - 18 febbraio 2001, n.71. Nello stesso senso si veda AA.VV., Perché lo spam è un problema, in spin.it. Gli autori evidenziano come uno «spammer, nell'arco di qualche ora, può facilmente raggiungere milioni di destinatari, utilizzando qualche centinaio o migliaio di macchine-relay (si tratta di computer non adeguatamente protetti che vengono utilizzati per inviare un maggior numero di messaggi ndA) di ignare «terze parti» per moltiplicare il numero di indirizzi raggiunti.

Di conseguenza, i costi globali associati alla distribuzione di uno spam possono essere molto elevati. Si è calcolato che la distribuzione di un tipico spam ha un costo di alcune centinaia di milioni o addirittura di miliardi di lire. Le componenti coinvolte sono molteplici:

- Il tempo perduto dai destinatari per scaricare, verificare e cancellare il messaggio. Ad esempio, cinque secondi moltiplicato per un milione di destinatari corrisponde a 1400 ore di lavoro;

2. Una definizione di *SPAM*

Prima di procedere oltre si rende necessario arrivare ad una definizione di *spam* che sia il più precisa ed univoca possibile. Per tale ragione si ritiene opportuno adottare la definizione proposta dalla maggior parte degli operatori *internet*:

«Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content[6]».

In primis è necessario chiarire cosa si intenda con «*unsolicited messages*» e, a tal fine, è indispensabile specificare «che cosa costituisce una evidente ed esplicita sollecitazione a comunicare rivolta ad altri, e che cosa no[7]».

A tal proposito sembra quasi superfluo sottolineare come non si possa, e non si debba, prescindere dal principio civilistico della buona fede: un'esplicita sollecitazione a ricevere comunicazioni di posta elettronica viene inviata dall'utente in maniera *deliberata* e palesemente volontaria, per esempio richiedendo informazioni ad un sito o richiedendo espressamente di essere iscritti ad una *mailing list*.

- I costi di banda sostenuti da Isp e utenti (collegamento via telefono) per il trasporto del messaggio. Ad esempio, 10kB moltiplicato per un milione corrisponde a 10GB di dati, il cui transito prende circa 20 giorni di tempo-linea assumendo una velocità media di 6kB/s;

- I danni (sia quelli diretti sui sistemi che quelli indiretti dovuti alle malfunzionamenti) causati dalle congestioni indotte dallo spam, soprattutto per chi ha la sventura di avere una macchina nella propria rete utilizzata come relay da uno spammer per invio massivo di Uce.

Chi sostiene questi costi? Non certo lo spammer, che al massimo perderà un account su un Isp «consumer». I costi dello spam sono sostenuti dagli utenti che li ricevono, e dagli Isp, che vedono aumentare i loro costi di gestione (banda e tempo-uomo), e alla fine dovranno scaricare questi costi sui canoni. Negli Usa questa cifra è stata quantificata in circa $25 annui per utente (1998). Un recente studio della Commissione Europea stima il costo globale dello spam in circa 10 miliardi di Euro annui, corrispondenti a circa il dieci per cento del costo operazionale globale di Internet».

[6] Tale definizione è tratta dal sito monkeys.com (http://www.monkeys.com/spam-defined/).

[7] In tal senso si veda AA.VV., *Definizione di spam*, pubblicato in internet presso il sito spin.it.

Tuttavia non di rado è accaduto che, per motivazioni politiche, economiche, o religiose, si sia tentato di estendere la definizione di «sollecitato» fino a ricomprendervi fattispecie completamente estranee alla sollecitazione stessa.

In particolare, d'accordo con uno dei principali siti italiani impegnati nel contrasto al fenomeno dello *spamming*[8], possiamo affermare che non costituisce sollecitazione a ricevere comunicazioni[9]:

- Una semplice visita ad un sito web[10];
- L'invio di un messaggio, o di un insieme di messaggi, da una persona ad un'altra o da una persona ad un forum di discussione pubblico, a meno che l'intento chiaro ed ovvio del messaggio originale sia quello di richiedere esattamente la ricezione di tali messaggi e purché siano state prese tutte le necessarie precauzioni per assicurarsi che il mittente della richiesta sia il titolare effettivo dell'indirizzo a cui verranno diretti i messaggi;
- La semplice esistenza di un forum di discussione pubblico, come un *newsgroup* USENET, una chat room, un canale IRC, o un *bulletin board system* (BBS), di per sé, non costituisce una sollecitazione verso alcuno ad inviare uno o più messaggi a quel forum pubblico come parte di una campagna di invio massivo, a meno che il possessore di quel forum (o il manutentore del relativo manifesto o FAQ, in assenza di un possessore chiaro) non abbia esplicitamente incoraggiato la trasmissione di messaggi inviati massivamente a quel forum;
- Una sollecitazione a ricevere un particolare tipo, categoria o classe di messaggi inviati massivamente (come ad esempio la richiesta di essere inseriti in un particolare mailing list gestito da una particolare entità) non costituisce una sollecitazione a ricevere qualsiasi altro tipo,

[8] Si tratta del sito web http://www.spin.it il cui *postmaster* Furio ERCOLESI è molto attivo nel contrasto allo *spam*.

[9] Il seguente elenco è stato tratto da AA.VV., *Definizione di* spam... *op.cit.*

[10] Utilizzando particolari accorgimenti è possibile acquisire l'indirizzo di posta elettronica dei visitatori di un sito a loro insaputa. In alternativa capita piuttosto di frequente che al navigatore venga richiesta una registrazione gratuita per poter accedere al sito. Detta registrazione in genere comprende anche l'indirizzo di posta elettronica.

categoria o classe di messaggi inviati massivamente, sia da parte dello stesso mittente che da altri mittenti;
- Una sollecitazione a ricevere un particolare tipo, categoria o classe di messaggi inviati massivamente non può mai essere effettuata da qualcuno per conto di terzi. Soltanto l'entità che riceverà i messaggi inviati massivamente può emettere una sollecitazione all'invio sul proprio indirizzo;
- Inserire il proprio indirizzo di posta elettronica in un luogo pubblicamente accessibile come una pagina *web*, un *newsgroup* USENET, un *bulletin board system* (BBS), o un record di registrazione di un dominio pubblicamente accessibile, *a meno che* la pubblicazione dell'indirizzo di contatto non sia accompagnata da una sollecitazione *chiara* ed *esplicita* da parte del possessore di quell'indirizzo a ricevere messaggi trasmessi in maniera massiva.

3. *E-MAIL* E PUBBLICI ELENCHI

In relazione a quest'ultimo punto deve osservarsi che in tal senso si è ripetutamente espresso anche il Garante della *Privacy*[11], di recente nella

[11] Il Garante si è spesso espresso con fermezza circa l'inutilizzabilità degli indirizzi di posta elettronica raccolti da newsgroup e mailing list. Si veda per esempio la Decisione dell'11 gennaio 2001 che, per la sua importanza, si riproduce qui integralmente: «1. In data 15 novembre 2000 il Garante ha avviato accertamenti nei confronti dell'Associazione politica nazionale Lista Marco Pannella per verificare la liceità e la correttezza di alcuni trattamenti di dati relativi ad indirizzi di posta elettronica, in relazione a circa trenta segnalazioni che lamentano la ricezione non gradita di messaggi per via telematica per finalità di comunicazione politica. Diversi cittadini lamentano anche di aver ricevuto numerosi messaggi del medesimo contenuto in un arco ravvicinato di tempo. Altri hanno fatto invece presente che non è stato loro possibile cancellarsi dagli elenchi dei destinatari secondo le modalità indicate nelle e-mail non gradite, o di essere stati costretti a reiterare invano più richieste di cancellazione. L'Associazione ha fornito un riscontro alla richiesta di informazioni, all'esito del quale il Garante osserva quanto segue. 2. Le segnalazioni sono fondate. L'Associazione ha fatto presente di aver reperito oltre 390.000 indirizzi di posta elettronica a scopo di comunicazione politica utilizzando un *software* a disposizione di un terzo il quale archivierebbe indirizzi e-mail visualizzati su pagine web con suffissi ".it", ".org", ".com" e ".net" accessibili a chiunque in rete senza l'uso di *password* o di altri sistemi di protezione. La circostanza non ha trovato pieno riscontro in quanto, da accertamenti tecnici effettuati, in almeno otto casi non è stato possibile reperire in rete gli indirizzi di posta elettronica dei cittadini che hanno inviato una segnalazione. Non

newsletter 10-16 febbraio 2003 in cui si ribadisce che «gli indirizzi di posta elettronica non sono liberamente utilizzabili da chiunque per il

appare tuttavia rilevante approfondire tale aspetto. Infatti, anche ritenendo che pure questi otto indirizzi siano stati effettivamente raccolti mediante il *software* menzionato dall'Associazione, l'utilizzazione per finalità di comunicazione politica di tali indirizzi - e degli altri che sono stati invece reperiti in rete - non risulta comunque lecita e corretta. Contrariamente a quanto infatti argomentato dall'Associazione, gli indirizzi di posta elettronica dei segnalanti non provengono da «pubblici registri, elenchi, atti o documenti conoscibili da chiunque» (art. 12, comma 1, lett. c), della legge n. 675/1996) e la loro utilizzazione nel caso in esame non è quindi consentita in mancanza di una previa manifestazione positiva di consenso da parte degli interessati (essendo altresì inoperanti gli ulteriori presupposti elencati nell'art. 12 della medesima legge). La previsione contenuta nella citata lettera c) non si riferisce a qualunque dato personale che sia di fatto consultabile da una pluralità di persone, ma ai soli dati personali che oltre ad essere desunti da registri, elenchi, atti o documenti «pubblici» (in particolare in quanto formati o tenuti da uno o più soggetti pubblici), siano sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque, regime che può peraltro prevedere modalità o limiti temporali i quali vanno rispettati anche in caso di comunicazione o diffusione dei dati (art. 20, comma 1, lett. b), legge n. 675/1996). Le citate disposizioni contenute negli artt. 12 e 20 della legge n. 675/1996, di cui è chiaro il significato letterale, possono essere semmai applicate in altri casi di stretta analogia in cui un determinato registro, elenco, atto o documento sia reso ad esempio accessibile a chiunque sulla base della determinazione di un soggetto pubblico adottata in base ad una norma (si veda ad esempio l'elenco degli abbonati al servizio di telefonia vocale, per il quale l'Autorità per le garanzie nelle comunicazioni provvede affinché sia reso disponibile agli utenti: art. 17, comma 1, d.P.R. 19 settembre 1997, n. 318). Inoltre, una legittimazione all'utilizzazione pubblica di determinati dati può derivare anche dal consenso espresso degli interessati, manifestato in modo specifico ed informato. Al contrario, le citate disposizioni non possono essere estese arbitrariamente in contrasto con la relativa ratio. In particolare, sul piano sistematico, esse non possono essere applicate in modo da poter trattare liberamente qualsiasi dato personale di natura non sensibile in base alla sola circostanza che il dato sia stato conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti. Tale interpretazione, oltre a vanificare il sistema di garanzie introdotto dalla citata legge, risulta anche in aperto contrasto con la direttiva europea n. 95/46/CE del 24 ottobre 1995 nella parte attinente ai presupposti di liceità del trattamento (art. 7). L'utilizzazione per finalità di comunicazione politica degli indirizzi di posta elettronica dei segnalanti non poteva pertanto avvenire senza un preventivo consenso manifestato dagli interessati eventualmente anche nei confronti di più soggetti. Per nessuno dei cittadini che ha presentato la segnalazione è invece risultato dimostrato che l'interessato (al momento dell'attivazione del rapporto con il fornitore di servizi di telecomunicazioni o successivamente) abbia espresso il proprio consenso alla divulgazione e all'utilizzazione da parte

solo fatto di trovarsi in rete.

La vasta conoscibilità degli indirizzi *e-mail* che Internet consente, non

di chiunque del proprio indirizzo di posta elettronica. Non era pertanto corretto gravare l'utente dell'onere di chiedere all'Associazione di interrompere l'invio dei messaggi non richiesti. 3. È parimenti per un verso infondata e per un altro ininfluente la tesi secondo cui, con la partecipazione a forum e newsgroup, l'utente «decide di pubblicare (cioè direndere pubblico) il proprio indirizzo di posta elettronica» ed «è consapevole che quell'indirizzo, quel dato, potrà esser letto ed acquisito da chiunque si trovi a passare dalla pagina web interessata».

Va considerato infatti che la conoscenza di fatto degli indirizzi che si realizza in tali casi non può essere disgiunta dalla finalità per cui essa avviene. Contrasta, pertanto, con i principi di correttezza e finalità del trattamento raccogliere i dati che singoli utenti «lasciano» in un newsgroup, forum, ecc. solo per le finalità di specifica discussione su determinati temi, hobbies, ecc., ed utilizzarli per altri scopi che nulla hanno a che vedere -anche indirettamente- con l'argomento per il quale l'utente partecipa ad una discussione più o meno «pubblica» ed indica il proprio recapito e le proprie generalità (art. 9, comma 1, lett. b), legge n. 675/1996). Una puntuale conferma della non correttezza di tale modalità di trattamento è posta tra l'altro in evidenza nel parere n. 1/2000 che il Gruppo europeo delle autorità garanti per la protezione dei dati ha adottato il 3 febbraio 2000 in tema di reti e di commercio elettronico (pubblicato sul sito web del Garante www.garanteprivacy.it). Anche tale atto pone infatti in evidenza che il solo fatto della rinvenibilità di un indirizzo e-mail in uno spazio pubblico di Internet non comporta un uso libero dell'indirizzo stesso per mailing elettronici. Il principio in esso affermato vale, poi, per ogni tipo di uso sistematico di una pluralità di recapiti non riconducibile ad un uso personale (su quest'ultimo, si veda un altro provvedimento adottato in data odierna dal Garante, sempre in tema di posta elettronica). 4. Ad una conclusione analoga a quella indicata nei precedenti punti deve pervenirsi anche per ciò che riguarda altri casi oggetto di segnalazione, nei quali gli indirizzi di posta elettronica sono stati acquisiti dall'Associazione in quanto pubblicati su alcuni siti web per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale ed associativa. La pubblicità di alcuni indirizzi resi conoscibili attraverso tali siti va collegata anch'essa, infatti, agli scopi per cui essa si verifica, non potendosi sostenere, anche in tali casi, che i dati posti a disposizione del pubblico per circoscritte finalità siano liberamente utilizzabili per l'invio generalizzato di e-mail anche quando queste non abbiano un contenuto commerciale o pubblicitario. 5.Le segnalazioni sono infine fondate anche per ciò che riguarda le modalità di cancellazione dei dati. A prescindere dalla liceità o meno dell'utilizzazione dei dati, l'Associazione era tenuta a soddisfare senza ritardo le richieste di cancellazione ai sensi dell'art. 13 della legge n. 675/1996, curando un servizio attivo ed efficace di eliminazione degli indirizzi dei reclamanti. Il numero delle segnalazioni pervenute al riguardo (che lamentano l'inerzia dell'Associazione o l'inattività del meccanismo telematico predisposto) non sembra invece far ritenere che si sia trattato solo di un disguido occasionale.6. L'Associazione deve quindi astenersi dall'utilizzare ulteriormente i dati personali relativi agli utenti che non abbiano previamente manifestato un consenso alla loro utilizzazione per finalità di comunicazione politica, il che può ovviamente avvenire sia in occasione dell'attivazione del rapporto con il fornitore di servizi telematici, sia al momento della partecipazione ad un forum o *newsgroup* o in altra circostanza.

rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti *on line*. Gli indirizzi e-mail non sono, insomma, «pubblici» come possono essere quelli presenti sugli elenchi telefonici».

Il principio è stato ribadito dall'Autorità Garante, da ultimo con il provvedimeto del 29 maggio 2003[12], che ha affrontato in questi ultimi mesi diversi casi di utenti che avevano segnalato la pratica ormai diffusa di inviare *e-mail* commerciali ad indirizzi di posta elettronica raccolti in rete. Alle proteste degli utenti, le società che avevano inviato le *e-mail* rispondevano che non vi era stata alcuna violazione della *privacy* perché gli indirizzi erano stati reperiti su *Internet* (spesso attraverso appositi software) e che pertanto erano «*pubblici*».

Niente di più sbagliato, afferma l'Autorità. Gli indirizzi di posta elettronica non provengono, infatti, da pubblici registri, elenchi, atti o documenti formati o tenuti da uno o più soggetti pubblici e non sono sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque[13].

L'Associazione deve adottare inoltre ulteriori misure per dare effettivo seguito alle richieste di cancellazione dei dati già pervenute o che pervengano successivamente.

TUTTO CIO' PREMESSO IL GARANTE:

dichiara fondate le segnalazioni riguardanti l'Associazione politica nazionale Lista Marco Pannella nei termini di cui in motivazione e dispone che questa fornisca al Garante un riscontro sulle misure adottate entro il 5 marzo 2001, ai sensi dell'art. 32, comma 1, della legge n. 675/1996».

[12] Ma si veda, da ultimo, il provvedimento del 29 maggio 2003 in cui il Garante, riassumendo l'attività sino ad oggi svolta contro il fenomeno dello spam presenta le seguenti conclusioni:

«TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 31, comma 1, lett. l) della legge 31 dicembre 1996, n. 675, vieta l'ulteriore trattamento illecito di dati personali realizzato a scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, effettuato in violazione delle disposizioni sopra richiamate da parte dei soggetti cui si riferiscono le segnalazioni e i reclami pervenuti;

2. ai sensi dell'art. 31, comma 1, lett. c) della legge 31 dicembre 1996, n. 675, segnala ai titolari del trattamento di cui agli atti del procedimento la necessità di conformare i trattamenti di dati personali ai principi richiamati nel presente provvedimento».

[13] Cfr provvedimento 29 maggio 2003: «Questa Autorità si è pronunciata più volte in materia ribadendo che la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari (cfr., ra l'altro, la decisione dell'11 gennaio 2001 - in Bollettino del Garante n. 16). In particolare, i dati dei singoli utenti che prendono parte a gruppi di

La circostanza che l'indirizzo *e-mail* sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti non lo rende, infatti, liberamente utilizzabile e non autorizza comunque l'invio di informazioni, di qualunque genere, anche se non specificamente a carattere commerciale o promozionale, senza un preventivo consenso.

L'Autorità garante sottolinea che l'eventuale disponibilità in *Internet* di indirizzi di posta elettronica, anche se resi conoscibili dagli interessati per certi scopi (ad esempio su un sito istituzionale o anche aziendale) attraverso siti *web* o *newsgroup*, va «*rapportata alle finalità per cui essi sono pubblicati sulla rete*».

A maggior ragione, quindi, questo principio deve valere in caso di uso indebito di software che rastrellano automaticamente migliaia di indirizzi in rete o li creano «*a tavolino*» a prescindere da un accertamento sulla loro effettiva esistenza.

Una considerazione a parte deve, infine, essere fatta in relazione a *postmaster*, *abuse*, *security* ed altri simili indirizzi di ruolo designati, su indicazione delle RFC *Internet* rilevanti oppure dai gestori od operatori di un server o di una rete, come indirizzi aventi lo scopo di ricevere comunicazioni relative all'operazione e/o alla manutenzione del *server* o della rete, ai mittenti dovrebbe essere lasciata la più ampia libertà rispetto alla questione della *sollecitazione* delle comunicazioni.

Si concorda che, per i messaggi elettronici diretti a tali indirizzi di

discussione in Internet sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico (art. 9, comma 1, lettere a) e b), legge n. 675). Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista «anagrafica» degli abbonati ad 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. 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. In quest'ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n. 675) e non anche a rendere l'interessato disponibile all'invio di messaggi pubblicitari)».

ruolo, un singolo pacchetto di qualsiasi tipo spedito dalla rete o dal server in cui si trova l'indirizzo in questione (a meno che non sia semplicemente una risposta a qualche pacchetto precedente) a qualche altro server o rete può essere considerato come una forma di sollecitazione, da parte del server o della rete che li emette verso la persona, server o rete che li riceve (o al relativo amministratore) per ulteriori comunicazioni, purché pertinenti, dirette a qualsiasi o a tutti gli indirizzi di ruolo associati con il server o rete che ha inviato il pacchetto[14].

Tuttavia, sebbene la casistica indicata e lo sviluppo dei concetti relativi al termine «sollecitato» e «non sollecitato» qui effettuata possa sembrare un mero esercizio di scuola, essendo la questione puramente di buon senso, la stessa è di notevole importanza soprattutto al fine di evitare che gli *spammers* - come spesso accade - possano affermare che questa distinzione è difficile da applicare alla realtà.

Non di rado capita di ricevere messaggi del tipo «Mi ha spedito una richiesta di informazioni, e pertanto ho inserito il suo indirizzo nel nostro *mailing list*», oppure «Il suo indirizzo *e-mail* appare sul suo sito *web* pubblicamente accessibile, quindi è aperto a comunicazioni da parte di chiunque», o ancora «Qualcun altro, forse uno dei suoi familiari, deve aver iscritto il suo indirizzo al nostro *mailing list*».

Deve invece ribadirsi, se mai ce ne fosse bisogno, che, a meno che non vi sia il consenso espresso in maniera esplicita dal destinatario stesso, qualsiasi messaggio spedito a quel destinatario deve essere, per definizione, ritenuto non sollecitato.

Se il messaggio suddetto è anche una componente di un processo o campagna di messaggi spediti massivamente, allora il mittente è uno *spammer* e sta effettuando un atto di *spamming*[15].

[14] In tal senso AA.VV., *Definizione di spam ... op.cit.*

[15] In tal senso si veda anche la decisione del 20 marzo 2002, del Garante della Privacy: «Nella fattispecie, analogamente a quanto rilevato in un altro caso esaminato da questa Autorità (provv. dell'11 gennaio 2001, in Bollettino del Garante n. 16, p. 39), l'indirizzo di posta elettronica del ricorrente non risulta provenire da «pubblici registri, elenchi, atti o documenti conoscibili da chiunque» e contenenti dati che possono essere quindi utilizzati, sia pure sulla base di un'idonea informativa, in mancanza di una manifestazione positiva di

4. I danni causati dallo *spam*

Il fenomeno è, poi, più diffuso di quanto non si creda: tanto per avere un'idea concreta delle sue reali dimensioni si consideri che oggi più di un'*e-mail* su due costituisce *spam*[16] e che la tipologia dei messaggi varia grandemente in base a molteplici fattori[17].

Non può poi trascurarsi che la presenza di tali messaggi nella casella di posta elettronica potrebbe pregiudicare gravemente la ricezione di altri messaggi molto più importanti in quanto ogni soggetto ha a propria disposizione uno spazio limitato in cui viene archiviata la posta in attesa che questa venga scaricata e letta dall'utente.

Tale spazio, generalmente più che sufficiente per le normali esigenze, potrebbe facilmente essere saturato a causa dell'accumulo di messaggi pubblicitari in caso di impossibilità di controlli per periodi medio-lunghi ovvero in caso di messaggi di *spam* particolarmente «*ingombranti*»[18].

consenso degli interessati (art. 12, comma 1, lett. c), legge n. 675/1996). La società resistente si è limitata ad indicare l'asserita origine dei dati (che sarebbero stati acquisiti da Labels Internet Services), ma non ha fornito alcun elemento che possa indurre a ritenere che nella fattispecie fosse stato manifestato un consenso per l'invio della e-mail contenente un'offerta di hosting per un dominio web, oppure operasse uno degli altri presupposti del trattamento equipollenti al consenso, elencati nel citato art. 12 della legge n. 675. Deve quindi ritenersi fondata la richiesta del ricorrente di vedere interrotta l'utilizzazione dei dati che lo riguardano, in applicazione della legge n. 675/1996 in relazione all'art. 10, comma 2, del d.lg. 13 maggio 1998, n. 171, nonché dell'invocato art. 10 del d.lg. 22 maggio 1999, n. 185 sulla protezione dei consumatori nei contratti a distanza, il quale vieta l'impiego della posta elettronica da parte di un fornitore senza il consenso preventivo del consumatore in relazione a determinate finalità tra cui rientrano quelle perseguite nel caso di specie. Il ricorrente ha formulato le proprie richieste ai sensi dell'art. 13 anche come diffida all'eventuale, ulteriore trattamento dei dati comunque in possesso della società (la quale asserisce peraltro di aver da ultimo cancellato il nominativo del ricorrente «dalle proprie liste») e per questo aspetto il ricorso va pertanto accolto ordinando alla società resistente di astenersi da ogni ulteriore trattamento dei dati personali relativi all'interessato e, in particolare, all' indirizzo di posta elettronica, in assenza di idonea manifestazione di consenso o di altro idoneo requisito ai sensi degli artt. 12 e 20 della legge n. 675/1996».

16 La stima precisa si aggira intorno al 60-65% dei messaggi ricevuti ed è visibile in Internet presso i seguenti siti: postini (http://www.postini.com/stats/index.html) e rhyolite (http://www.rhyolite.com/anti-spam/dcc/graphs/).

17 Si veda sempre http://www.rhyolite.com/anti-spam/dcc/graphs/comp-rates?resol=1month.

18 Cfr. A. Monti, *Opt-out: il galateo invertito dello spam builder*, in interlex.it, 19/07/01.

A ciò deve aggiungersi che, in una casella piena di *spam*, diventa oltremodo difficoltoso effettuare una cernita tra i messaggi utili e la spazzatura: non di rado può capitare che un messaggio importante sfugga, o venga cancellato!, perché l'attenzione è rivolta a rimuovere le varie «irresistibili» offerte[19].

Occorre poi osservare che, sebbene di regola i messaggi di *spamming* siano piuttosto piccoli, in genere inferiori ai 20Kb, come sempre ci sono delle eccezioni: si sta, infatti, diffondendo la moda di inviare *e-mail* contenti immagini oppure «dialer» (il classico è «c'è una cartolina per te» o «vieni a conoscermi!») che superano abbondantemente i 50Kb, ma, soprattutto, rischiano di indurre gli utenti più ingenui ad effettuare connessioni non desiderate e piuttosto care (1,5 o 2 euro al minuto!).

Non può poi tacersi che spesso si tratta di messaggi inviati da gestori di siti contenenti materiale pornografico, o addirittura pedo pornografico, con contenuto quasi sempre volgare, che potrebbe facilmente ferire la sensibilità di moltissimi soggetti (per non parlare della necessaria tutela dei minori dai contenuti illeciti o nocivi); nelle altre occasioni si tratta quasi sempre di palesi truffe[20], di fantasiose catene di Sant'Antonio, di

[19] In tal senso si veda anche quanto affermato dal Garante della Privacy nel provvedimento del 29 maggio 2003 in cui si ribadisce che «… l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad adottare «filtri», a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico. Il fenomeno interessa anche piccole e grandi imprese destinatarie di un elevato numero di messaggi, le quali devono farsi carico di misure interne e di costi anche organizzativi per contrastarlo. Questo ingiustificato riversamento sugli utenti dei costi pubblicitari si verifica anche relativamente a messaggi inviati da singole persone fisiche che, in vari casi esaminati, non si limitano ad una comunicazione episodica, ma intraprendono una comunicazione sistematica per fini personali o, addirittura, una diffusione di dati cui è applicabile la disciplina in materia di protezione dei dati personali (art. 3 legge n. 675)».

[20] Classico l'esempio dello *spam* nigeriano (o 419, dal numero della legge antitruffa nigeriana) in cui un sedicente ministro, ex ministro o possidente nigeriano chiede al destinatario di aiutarlo ad esportare dal suo paese del denaro, più o meno legittimamente posseduto. Il testo del messaggio generalmente varia (ne esistono differenti versioni), ma il contenuto è

finti allarmi virus, di incredibili offerte di diplomi e titoli accademici etc.

Resta in ogni caso opportuno sottolineare che lo *spam* è negativo indipendentemente dal suo contenuto, non necessariamente commerciale o illegale[21].

A tale proposito è evidente che, trattandosi di una pratica piuttosto fastidiosa viene abitualmente evitata dalle ditte più serie che, con tale sistema, rischierebbero di squalificarsi agli occhi dei consumatori, tanto che si è andata affermando la prassi di inviare falsi messaggi di *spam* apparentemente generati da un soggetto al solo fine di screditarlo agli occhi dei destinatari del messaggio[22].

5. I MEZZI DI DIFESA

Al fine di difendersi dall'ondata di messaggi, già da tempo, utenti e *provider* hanno attuato una politica di ostracismo nei confronti degli *spammer* negando loro accessi e servizi; il sistema più efficace consiste nella compilazione di liste (cosiddette *black list*) in cui vengono inseriti gli *spammer* e, soprattutto, i riferimenti dei *provider* accusati di favoreggiamento nei confronti di questi soggetti.

sempre il medesimo: si chiede al destinatario di fornire gli estremi del suo conto corrente dove effettuare un ingente bonifico. In cambio del disturbo allo stesso viene promessa un'ingente quota del denaro.

[21] *Crf.* la Decisione dell'11 gennaio 2001, riportata *infra*, in cui il contenuto del messaggio era di propaganda politica.

[22] Si tratta del cd *joe job*. Con questo termine si indica la prassi di inviare messaggi di *spam* fingendo che provengano da un altro mittente. In questo modo si può ottenere un duplice scopo: in primis non si viene coinvolti nel traffico generato dallo *spam*, sia in termini di messaggi di *delivery failure* che in termini di proteste degli utenti raggiunti vittime dello *spam* ed in secondo luogo si riduce la possibilità di vedersi revocare l'account dal proprio *provider*. Si raggiunge inoltre lo scopo di danneggiare gravemente l'immagine del soggetto coinvolto nel *joe job* screditandolo e mettendolo in pessima luce di fronte alla comunità informatica. La pratica, infatti, viene spesso posta in essere contro soggetti particolarmente attivi nella lotta allo *spam* o ad altre forme di criminalità mentre altre volte vengono presi di mira soggetti scelti a caso ovvero reti con errori di configurazione relativamente al *server* smtp. Da un punto di vista giuridico l'autore del *joe job* commette il reato previsto e punito dall'articolo 617-*sexies,* del codice penale in quanto forma falsamente una comunicazione relativa ad un sistema telematico anche se in talune circostanze potrebbe ravvisarsi un concorso con altre fattispecie criminali.

Occorre, in primo luogo, sottolineare che queste liste non hanno alcun carattere di ufficialità e che vengono volontariamente adottate da coloro che decidono di farne uso, pertanto la loro diffusione è dovuta esclusivamente all'affidabilità delle stesse e del loro *mantainer*.

Una delle liste più note è quella realizzata da SPEWS, *Spam Prevention Early Warning System*, un'organizzazione i cui gestori sono praticamente invisibili e non comunicano con l'esterno in nessun modo se non tramite il sito web.

Veniamo a spiegare come funziona in concreto il sistema utilizzato da SPEWS e perché lo stesso deve essere ritenuto pienamente legittimo. In primo luogo osserviamo subito che se un *provider* viene inserito in una *black list* vi è si solito una buona ragione; in genere vuol dire che ospita un sito *spam-advertised*[23], è egli stesso veicolo di *spam*[24], o comunque non interviene nonostante proteste e segnalazioni.

In parole povere il solo fatto di ospitare uno *spammer* non comporta nessun rischio di finire automaticamente in una black list, sempre che la fornitura di servizi venga sospesa in seguito a segnalazioni e purché l'intervento venga effettuato in tempi rapidi.

Nel caso in cui non vengano adottate adeguate misure nei confronti dello *spammer*[25] la prassi è quella di iniziare bloccando soltanto l'indirizzo IP contenente il sito dello *spammer* e, se lo stesso provider ne ha altri e continua a non prendere provvedimenti, il blocco viene progressivamente allargato fino a coprire tutti i suoi clienti.

In alcuni casi, se lo *spammer* è particolarmente attivo, è possibile che

[23] Con tale termine si indica un sito web che viene promosso attraverso l'invio massiccio ed indiscriminato del proprio URL o della propria *home page*.

[24] È veicolo di *spam* sia il provider che non prende provvedimenti nei confronti dei propri utenti accusati di *spamming* sia il provider che, non configurando adeguatamente i propri sistemi. consente a chiunque di inviare messaggi attraverso il proprio server smtp. In quest'ultimo caso si parla più propriamente di «*open relay*». Tali servizi possono essere volontari (in tal caso, spesso i gestori di tali servizi non tollerano che gli stessi vengano utilizzati per inviare spam e, pertanto, adottano idonee misure di sicurezza al fine di impedirne un utilizzo illecito) o involontari (errore nella configurazione dei servizi).

[25] Vi è poi il caso il cui il *provider* stesso è uno *spammer*, il che, generalmente, significa un'ammonizione seguita, nel caso in cui lo *spammer* perseveri, dalla disabilitazione dell'*account* e, in caso di siti internet *spam advertised*, dall'oscuramento del sito.

si inizi direttamente bloccando una rete più grande.

Nel caso di SPEWS questi indirizzi sono contenuti nella lista di livello 1, accessibile tramite la DNSBL[26] di osirusoft.com, tuttavia vi è anche una lista di livello 2 che è possibile scaricare dal sito e che usa criteri decisamente più aggressivi.

In sintesi, per un *provider* l'inserimento nel livello 2 rappresenta un segnale, consultabile anche con metodi automatici, che il suo *abuse desk*[27] non funziona in modo adeguato.

Una volta che si è stati inseriti in SPEWS, per essere rimossi è sufficiente scrivere sul gruppo di discussione *news.admin.net-abuse.email* dopo aver preso provvedimenti nei confronti dello *spammer*; in alternativa, trascorso un certo periodo di tempo, se lo *spammer* cessa la sua attività e nessuno si lamenta più, i gestori prima riducono il livello e poi tolgono il *provider* dalla *black list*, ma in questa seconda ipotesi per ottenere la «riabilitazione» possono essere necessari parecchi mesi.

Il sistema è estremamente efficace in quanto, di fatto, costringe i *provider* ad una non facile scelta: combattere attivamente lo *spam* o vedersi respingere tutti i messaggi provenienti dai propri utenti con conseguente probabile migrazione degli stessi verso un altro provider che offra maggiori garanzie di serietà.

Naturalmente, preso atto dell'efficacia dello strumento, vi è stato subito chi, autoproclamatosi paladino di non si sa bene quali diritti, ha innalzato la propria vibrante protesta, giungendo a scomodare persino la Carta Costituzionale e paventando che «potremmo vederci tolto il diritto alla corrispondenza virtuale[28]».

L'argomento preferito dai critici di SPEWS è quello secondo cui le *black list* colpirebbero anche innocui navigatori in quanto «la particolarità del

[26] *Domain Name System Black List*: si tratta di liste di indirizzi Internet comunemente usati dagli *spammers*; rifiutando tutte le e-mail provenienti da questi indirizzi è possibile bloccare una grossa quantità di *spam*.

[27] L'*abuse desk* è un servizio, che tutti i *provider* dovrebbero avere, deputato a conoscere e ad analizzare le segnalazioni di abuso di servizio (*spam*, ma non solo) commesse dagli utenti di un determinato *provider*. In genere *l'abuse* è il biglietto da visita del provider e la cartina di tornasole in grado di indicare la sua serietà nei confronti delle violazioni alla netiquette o degli altri illeciti commessi dagli utenti di un servizio.

[28] Cfr. G.A. CAVALIERE, *Antispam: con Spews al bando il diritto alla e-mail!*, in vnunet.it.

funzionamento di questa nuova comunità *anti-spam* consiste in particolar modo nell'estendere le attività di «oscuramento» (c.d. *blacklisting),* oltre a chi fa *spamming,* anche ai soggetti che non sono *spammers.*

Questi ultimi, infatti, possono essere anche dei semplici, innocui navigatori, ma hanno la sfortuna di essere - loro malgrado - clienti di quegli ISP che si rifiutano di bloccare lo spam che producono in rete, pur dietro segnalazione dello SPEWS stesso di interrompere le attività di disturbo[29]».

La realtà dei fatti è ben diversa: *SPEWS*, come altri sistemi simili, non effettua alcuna azione diretta nei confronti degli *spammer*, limitandosi a realizzare delle liste in cui vengono indicati gli indirizzi IP utilizzati dagli *spammer*.

Tali liste vengono poi volontariamente adottate dai *provider* consapevoli della loro altissima affidabilità. Non può poi trascurarsi che si tratta di liste pubbliche e, pertanto, qualsiasi utente o «mite navigatore» che dir si voglia ha la concreta possibilità di consultarle verificando se il *provider* a cui intende rivolgersi è affidabile o meno.

Se tale verifica non viene effettuata non ci si può poi dolere delle conseguenze di una scelta poco ponderata; d'altra parte è noto che l'ignoranza di un fatto lesivo non può essere invocata a proprio favore da un soggetto se questa circostanza poteva (o doveva) essere conosciuta utilizzando l'ordinaria diligenza.

6. LA NORMATIVA IN MATERIA

Prima di procedere oltre, si rende necessario osservare che, sebbene ancora oggi in Italia manchi un corpus organico di disposizioni in materia, vi possono essere ben pochi dubbi in merito all'illiceità, anche penale, dello *spam*[30].

[29] Cfr. G.A. CAVALIERE, *Antispam ... op.cit.*

[30] Ma si veda ora il D.Lgs 30 giugno 2003, n.196, art.130. In tal senso si era in precedenza espresso il Garante, nel corso del noto provvedimento del 29 maggio, osservando che lo spam, inteso come trattamento illecito di dati personali "è già vietato direttamente dalla legge, senza che sia necessario adottare uno specifico provvedimento interdittivo del Garante dell'autorità giudiziaria; determina, a seconda dei casi, l'applicazione di sanzioni amministrative pecuniarie, in particolare per omessa informativa od omessa notificazione (artt. 10, 34 e 39 legge n. 675; art. 12 d.lg. n. 185/1999)".

In *primis* è necessario osservare che la disciplina giuridica cui soggiace l'attività di marketing deve necessariamente muovere dall'analisi della Legge 675/1996[31].

Dal combinato disposto degli articoli da 11 a 14 della legge 675 si evince, infatti, che l'interessato deve manifestare il proprio consenso espresso al trattamento dei suoi dati personali dopo essere stato informato, per iscritto, in merito alle finalità, alle modalità del trattamento, alla natura obbligatoria o facoltativa del conferimento dei dati, alle conseguenze di un eventuale rifiuto di rispondere, etc.

Ciò, tuttavia, sembrerebbe[32] comportare l'autorizzazione ad inviare almeno un'*e-mail*, ma tale dubbio è stato recentemente sciolto dallo stesso Garante[33] il quale nel ricordare che «il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi» ha espressamente previsto che «tale disciplina non può essere elusa inviando una prima *e-mail* che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario, oppure riconoscendo solo un diritto di tipo c.d. «opt-out» al fine di non ricevere più messaggi dello tesso tenore».

Un deciso passo in avanti è stato, tuttavia, compiuto con il D.Lgs 171/98[34], che all'art. 10[35] vieta l'utilizzo, senza il preventivo, consenso dell'abbonato di un sistema automatizzato di chiamata senza intervento

[31] Cd «Legge sulla privacy».

[32] Cfr. A. MONTI, Opt-in, *ovvero la ricerca del contatto diretto* in interlex.it; M. MAGLIO, Scusi, ma lei è «optinist» o «optautista»?, in interlex.it; M. CAMMARATA, *La difficile difesa del diritto alla riservatezza*, in interlex.it; COMUNICATO STAMPA AIDIM, 12 luglio 2001.

[33] Cfr. provvedimento 29 maggio 2003.

[34] Decreto legislativo 13 maggio 1998, n. 171 (in Gazz. Uff., 3 giugno, n. 127) - Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, e in tema di attività giornalistica.

[35] Dlgs 171 del 1998, art.10 «Chiamate indesiderate. 1. L'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato. 2. Le chiamate per le finalità di cui al comma 1, effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 11 e 12 della legge».

di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta.

Infine, con il Decreto Legislativo 185/99[36], il legislatore ha, al primo comma dell'art.10[37], previsto in maniera espressa un sistema «opt-in»[38] in relazione alle *e-mail* pubblicitarie ed ad altre forme di comunicazione commerciale riservando il sistema «opt-out»[39] a tecniche di comunicazione a distanza diverse da quelle previste al comma 1 purché consentano una comunicazione individuale con il consumatore.

Di recente anche il Parlamento Europeo, ha espressamente vietato l'invio di *e-mail* a carattere promozionale in assenza di preventivo consenso dell'interessato, prevedendo infine che «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[40]».

Da ultimo, il 30 giugno 2003, l'intera disciplina in materia di *privacy* è

[36] Decreto legislativo 22 maggio 1999, n. 185 in Gazz. Uff., 21 giugno, n. 143) - Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza.

[37] D.lgs 185 del 1999, art.10: «Limiti all'impiego di talune tecniche di comunicazione a distanza.

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».

[38] L'utente deve autorizzare preventivamente l'invio di messaggi commerciali.

[39] Le comunicazioni commerciali possono essere inviate, senza autorizzazione del destinatario, finché l'interessato non si oppone.

[40] Articolo 13 della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, Relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, GUCE n. L 201 del 31/7/2002:

«Articolo 13 - Comunicazioni indesiderate

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

stata accorpata nel cosiddetto «Codice in materia di protezione dei dati personali[41]» il cui articolo 130 regolamenta espressamente l'utilizzo della posta elettronica, e di altre tecnologie, a fini pubblicitari vietandolo senza l'espresso consenso del destinatario.

Possiamo, quindi, affermare senza tema di smentite che lo *spam* costituisce un illecito per il nostro ordinamento, soprattutto quando effettuato con determinate modalità.

7. Liceità delle cd *Black List*

La difesa ad oltranza degli spammer, tuttavia, finge di ignorare il suddetto particolare passando al contrattacco e giungendo ad affermare che l'adozione di filtri e black list deve essere ritenuta illecita in quanto lesiva del diritto, costituzionalmente garantito, alla riservatezza della corrispondenza ed all'espressione delle proprie opinioni.

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».

[41] Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, pubblicato in Gazz.Uff. n. 174 del 29-7-2003 - Suppl. Ord.n.123 – e destinato ad entrare in vigore dal 1-1-2004.

Giova, a questo punto, osservare che una simile difesa è palesemente illogica, se non in malafede: l'articolo 15 della costituzione tutela, infatti, «*l*a libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione», ma non occorre attendere una pronuncia della Consulta per capire che i messaggi pubblicitari, inviati in modo massiccio ed indiscriminato, non possono certo essere definiti corrispondenza; in caso contrario assisteremmo all'arresto ed alla successiva condanna di un buon 90% dei portieri dei nostri condomini, usi a raccogliere e gettare, senza tanti complimenti, i volantini pubblicitari che infestano le nostre cassette delle lettere.

Non tutte le comunicazioni sono *ipso facto* «corrispondenza», ma soltanto quelle che possiedono alcuni requisiti individuati da dottrina e giurisprudenza in primis il requisito della personalità.

A tale proposito deve osservarsi, in via preliminare, che, nel nostro ordinamento, le comunicazioni commerciali non trovano tutela ai sensi dell'articolo 21 della Costituzione, ma, piuttosto, ai sensi dell'articolo 41 della Carta Costituzionale con le inevitabili differenze nel bilanciamento con il diritto alla tutela della vita privata e dei diritti individuali dei cittadini (soprattutto alla luce dell'art. 41, comma 2, Cost.[42]).

Ciò premesso, non può, poi, sfuggire che, in generale, chi utilizza una *black list* a livello di server nega il transito del messaggio prima che questo avvenga, impedendone l'accesso al sistema ed agendo su caratteristiche in grado di identificare in maniera affidabile il sistema mittente (e quindi non il soggetto mittente).

Per tale ragione, la segretezza della corrispondenza non può assolutamente venire in alcun modo compromessa in quanto nemmeno un bit giunge nel sistema ricevente.

Osserviamo poi *ad abundantiam* che il D.Lgs 74 del 1992[43] definisce pubblicità «qualsiasi forma di messaggio che sia diffuso in qualsiasi modo, nell'esercizio di una attività commerciale, industriale, artigianale o

[42] In tal senso si veda quanto affermato da A. Putignani, *Consenso, informativa e direct marketing – 1*, in Interlex.

[43] Decreto legislativo 25 gennaio 1992, n. 74 (in Suppl. ordinario alla Gazz. Uff., 13 febbraio, n. 36). - Attuazione della direttiva 84/450/Cee, come modificata dalla direttiva 97/55/CE in materia di pubblicità ingannevole e comparativa.

professionale allo scopo di promuovere la vendita di beni mobili o immobili; la costituzione o il trasferimento di diritti e obblighi su di essi oppure la prestazione di opere e servizi»[44].

Non vi è dunque dubbio che lo *spam* possa essere ricondotto alla pubblicità, ma questa, tuttavia, incontra dei limiti ben precisi; in particolare la legge 223/90[45] contiene diverse disposizioni che, pur essendo state dettate per la pubblicità televisiva, possono essere estese anche alla pubblicità via *Internet*.

In particolare l'articolo 8 della suddetta legge stabilisce che la pubblicità «non deve offendere la dignità della persona, non deve evocare discriminazioni di razza, sesso e nazionalità, non deve offendere convinzioni religiose e ideali, non deve indurre a comportamenti pregiudizievoli per la salute, la sicurezza e l'ambiente, non deve arrecare pregiudizio morale o fisico a minorenni».

La pubblicità incontra, quindi dei limiti piuttosto rigidi che già metterebbero fuori legge una buona percentuale dello *spamming* quotidiano; a ciò poi deve aggiungere che la Camera di Commercio Internazionale ha predisposto nel 1996 delle «*Guidelines on interactive marketing communications*» con lo scopo di sviluppare la fiducia degli utenti di *Internet* nei servizi della rete rendendo gli stessi più sicuri e trasparenti; in particolare i punti principali di tali guide, che rappresentano una sorta di *netiquette* per la pubblicità in rete, prevedono tra l'altro il diritto di non ricevere messaggi non richiesti.

Dello stesso avviso è anche la Corte Suprema degli Stati Uniti che, in tutta una serie di recenti decisioni[46], ha stabilito che non sussiste alcun diritto di inviare *spam*:

«Cyber Promotions, Inc. does not have a right under the First Amendment to the United States Constitution or under the Constitutions of Pennsylvania and Virginia to send unsolicited e-mail advertisements over the Internet to members of American Online, Inc.

[44] Dlgs 74 del 1992 art. 2.

[45] Legge 6 agosto 1990, n. 223 (in Gazz. Uff., 9 agosto, n. 185). Disciplina del sistema radiotelevisivo pubblico e privato.

[46] Cfr. AOL V, *Cyberpromo*8, *Concentric Networks v. Cyberpromo9, Earthlink v. Cyberpromo*10 etc.

and, as a result, American Online, Inc. may block any attempts by Cyber Promotions, Inc. to do so».

Non può, infine, tacersi che il diritto alla riservatezza della corrispondenza è un diritto disponibile e che come tale il soggetto titolare può validamente rinunciarvi in parte o in tutto; indicativa in tal senso è la punibilità solo su querela di parte, mentre chiaramente non può inferirsi dall'inviolabilità di cui all'art.15 primo comma Cost. alcun senso di indisponibilità (come pure in molti nell'ambiente telematico hanno tentato).

Detta rinuncia può essere *erga omnes*, ed in tal caso la corrispondenza diviene pubblica, oppure limitata nei confronti di alcuni soggetti e per determinati scopi, come, per esempio, avviene piuttosto spesso nei confronti del provider al fine di evitare messaggi di *spam*.

La rinuncia può essere espressa, nell'ipotesi in cui l'utente accetti, o richieda, espressamente una qualche forma di controllo, ma anche tacita quando un simile comportamento costituisce una prassi diffusa e comunemente accettata, anzi spesso incentivata, nei rapporti tra utenti e provider come, per esempio, nel caso di protezione antivirus ed anti*spam* predisposta dai provider[47].

È, comunque, necessario sottolineare che, almeno finché non si formerà una precisa giurisprudenza in tal senso, i fornitori di servizio prevedano espressamente in sede contrattuale l'utilizzo delle *black list*, al fine di non incorrere in sanzioni civili e penali in seguito alla mancata consegna della corrispondenza ai propri utenti[48].

[47] A tale proposito si veda quanto affermato dal Tribunale di Prato, 15 ottobre 2001, secondo cui «Il contratto tra l'utente (titolare di solo indirizzo di posta elettronica e/o di sito web) ed un soggetto che svolga attività di provider, ha la natura di appalto di servizi. Conseguentemente rientra tra i doveri collaterali gravanti sul provider anche quello di evitare che il proprio utente di posta elettronica sia esposto ad un'attività di invio c.d. a pioggia («spamming») di messaggi e/o di materiali pubblicitari non graditi da parte di altri soggetti operanti nella rete».

[48] Cfr. Tribunale di Prato, 15 ottobre 2001. «Il provider che impedisca che determinati messaggi di posta elettronica raggiungano gli iscritti facenti parte di un altrui «maillist» pone in essere (oltre che una violazione degli obblighi contrattuali verso il proprio utente di posta elettronica, anche) un illecito nei confronti dell'impresa emittente. Tale attività di blocco può ritenersi svolta «iure», cioè conformemente al diritto, solo se giustificata dall'adempimento di un'obbligazione contrattuale».

Da ultimo giova osservare che l'articolo 130, 6° comma, del D.Lgs 196 del 2003 prevede espressamene che «in caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni».

Di fatto si tratterebbe soltanto di attendere un provvedimento del garante per rendere «operative» le *black list* in quanto non vi è dubbio che il legislatore, adoperando la definizione «coordinate di posta elettronica» non ha fatto riferimento soltanto agli indirizzi di posta elettronica, ma anche a tutti quegli elementi, ivi compresi gli indirizzi IP di origine, che possano essere validamente utilizzati per difendere efficacemente la *privacy* dei cittadini che navigano in *Internet*.

«Ove il limite e la cernita dei messaggi inviati dal «provider» ai propri utenti non risultino imposti dalle pattuizioni «inter partes», interpretate alla stregua dei principi generali ex art. 1175 e 1375 c.c., appare non conforme alla correttezza professionale in confronto dell'impresa mittente - ai sensi dell'art. 2598 n. 3 c.c. - la condotta del «provider» il quale impedisca che determinati messaggi di posta elettronica raggiungano i propri utenti iscritti al sito donde i messaggi stessi provengano, e pertanto ne è consentita l'interdizione con misura d'urgenza ex art. 700 c.p.c.».