

La nuova normativa antispam australiana a confronto con gli obblighi dei providers italiani

Sommario: Introduzione. §1. Che cosa è lo Spam. §2.1 Australia: il Telecommunications Act 1997 e lo Spam Act 2003, §2.2 Le previsioni dell'Internet Industry Spam Code of Practice. §3. Le disposizioni comunitarie in tema di spamming e di comunicazioni elettroniche non desiderate. §4.1 Il quadro normativo italiano. §4.2. Le responsabilità degli Internet Service Providers Italiani. §5. Conclusioni.

Introduzione.

Nel presente contributo si analizza l'architettura normativa australiana e le soluzioni adottate in tema di *spam*, per poi proseguire nella comparazione con gli obblighi a carico degli Internet Provider e gli strumenti posti in essere dalla legislazione comunitaria e italiana nell'affrontare il problema delle comunicazioni di posta elettronica indesiderate.

§1. Che cosa è lo spam.

La pratica dello "spam"¹, o "spamming", è di difficile definizione²; in generale ci si riferisce a quella serie di comunicazioni di posta elettronica³, *newsgroups*,

¹ L'origine di tale locuzione deriva da un impasto di carne di maiale e prosciutto in scatola (*spicy pork and ham*) di qualità gastronomica molto bassa diffuso negli Stati Uniti. Questo prodotto fu oggetto di una famosa scenetta dei Monty Python ambientata in un ristorante dove tutti i piatti offerti contenevano tale ingrediente mentre gli avventori ordinavano ossessivamente lo spam (G. Livraghi, *I pericoli dello spamming*, consultato in Internet il 1 aprile 2006 sul sito web <http://gandalf.it/mercante/merca2.htm#heading04>; F. Di Ciommo, *Lo "spamming", dalle reti telematiche alle aule dei tribunali*, in *Foro. it.*, 2004, 2908). Da allora il termine *spam* è entrato nel linguaggio della quotidianità per indicare "tutto ciò che è di pessima qualità, cioè spazzatura, nonché per esprimere l'idea di un disturbo nella comunicazione di livello e continuità tali da renderla impossibile (P. Crugnola, *Disciplina dello spamming*, in *Nuova Giur. Civ. Comm.*, 2004, II, p. 474; A. Levi, F. Zanichelli, *L'utilizzo dell'e-mail a fini pubblicitari: dallo "spamming" al "permission marketing"*, in *Riv. dir. ind.*, 2001, I, 195, n. 3; E. O. Policella, *Il danno da spamming*, in *Danno e Resp.*, 2005, p. 66; C. Ercolano, *Spamming: una nuova forma di pubblicità dannosa per i consumatori?*, in *Diritto della Gestione Digitale delle Informazioni*, supplemento al n. 9 de *Il Nuovo Diritto*, 2002, p. 44; O. Sarlo, "Spamming", "mailing list" e tutela dei dati personali. Più garanzie dalle nuove decisioni dell'autorità garante, in *Dir. e Giust.*, 2003, fasc.10, p. 94). Secondo taluno, però, in questo contesto il termine "spam" si riferisce all'acronimo di *Send Phenomenal Amount of Mails*, ovvero "spedire una quantità fenomenale di posta elettronica" (M. A. Senor, *Comunicazioni indesiderate tecniche commerciali, spamming e consenso dell'interessato*, Relazione tenuta al convegno *I diversi aspetti del diritto alla protezione dei dati personali*, Torino, 10 maggio 2004, p. 5 del manoscritto). Gli esperti del settore distinguono due varianti di posta elettronica indesiderata: la *Unsolicited Commercial E-Mail (UCE)* e la *Unsolicited Bulk E-Mail (UBE)*. I messaggi appartenenti alla prima categoria sono caratterizzati dal contenuto commerciale di promozione di beni ovvero servizi; mentre quelli della seconda categoria si distinguono per essere messaggi singoli inviati ad un grande numero di destinatari (N. Lucchi, *Comunicazioni indesiderate: lo spamming tra razionalizzazione delle norme esistenti e pronunce dell'Autorità di Garanzia*, in *Studium Juris*, 2004, p. 457; D. E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, in *35 U.S.F. L. Rev.* 325 (2001), p. 328).

² S. I. Ahn, *Background Paper for the OECD Workshop on Spam*, DSTI/ICCP(2003)10/FINAL, pubblicato on line il 9 febbraio 2004 e consultato sul sito web [http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp\(2003\)10-final](http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final) in data 1 aprile 2006.

³ Il D. Lgs. 30 giugno 2003, n. 196 relativo al "Codice in materia di protezione dei dati personali" (pubblicato nella *Gazzetta Ufficiale* n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123) e

chatlines, SMS (*Short Message Service*) non richieste inviate da mittenti sconosciuti o con i quali non si ha un rapporto di corrispondenza abituale o istituzionale. Concretamente, lo *spamming* consiste nell'invio di messaggi in prevalenza pubblicitari⁴ o con altre finalità, come le catene di Sant'Antonio, propaganda politica, proselitismo religioso, pornografia, scommesse o invio di *worms*, *trojan horses*, *dialers*, *phishing* o virus destinati ad infettare il computer dell'incauto ricevente, onde assumere illegittimamente informazioni sulle abitudini di navigazione o addirittura il controllo⁵.

Le potenzialità pubblicitarie e di *marketing* di Internet sono note da tempo⁶ e la pratica dello *spamming* va posta in primo piano tra le molteplici modalità di utilizzo commerciale della Rete. Il costo minore delle campagne promozionali effettuate tramite posta elettronica, paragonato con le spese sostenute per quelle che utilizzino mezzi di comunicazione tradizionali, quali televisione, telefono o posta ordinaria, e un maggiore riscontro da parte della clientela⁷, spiegano la crescente diffusione dello *spamming* nel web.

In occasione della redazione dei lavori preparatori dello *Spam Act 2003*, il governo federale australiano incaricò il *National Office for the Information Economy* (NOIE) di effettuare uno studio approfondito sul tema. I risultati, pubblicati in Rete⁸, illustrano come i messaggi di *spam* presentino frequentemente caratteristiche comuni, quali la spedizione in maniera indiscriminata e ripetitiva spesso da software automatici di contenuti illegali, offensivi e fraudolenti in violazione delle normative a tutela della riservatezza dei dati personali e strutturati in modo da non poter risalire al vero mittente dei messaggi⁹. I messaggi di *spam*, inoltre, non offrono informazioni sulle modalità di cancellazione del proprio indirizzo dalla memoria del programma mittente¹⁰.

conosciuto come "Codice della Privacy" all'art. 4, lettera m) definisce "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza". In dottrina E. O. Policella, *Op. cit.*).

⁴ Sul problema della pubblicità in Rete, E. Grazzini, *La pubblicità nelle Reti*, in *Problemi dell'informazione*, 1996, p. 38; V. Zeno Zencovich, *La pubblicità nei servizi di telecomunicazioni*, in *Aida*, 1996, p. 256.

⁵ S. Gauthronet, E. Drouard, *Messaggi pubblicitari indesiderati e protezione dei dati personali*, consultato in data 1 aprile 2006 all'indirizzo web <http://www.privacy.it/aretespamm2001.html>; E. Florindi, *Spam e tutela della riservatezza*, in *Informatica e diritto*, 2003, II, p. 185; D. D'Agostini, *A che punto è la lotta allo spam?* in *Cyberspazio e diritto*, 2004, p. 217

⁶ Si veda in questo senso il provvedimento dell'Autorità garante per la concorrenza ed il mercato n. 4820 del 27 marzo 1997, in *Dir. inf. inf.*, 1997, p. 1064; in dottrina E. O. Policella, *Ult. Op. Loc. Cit.*

⁷ S. Gauthronet, E. Drouard, *Messaggi pubblicitari indesiderati*, cit.; E. O. Policella, *Ult. Op. Loc. Cit.*

⁸ Accessibili su http://www.dcita.gov.au/__data/assets/pdf_file/21064/SPAMreport.pdf, sito web consultato in data 1 aprile 2006.

⁹ La lotta allo *spamming* va condotta non soltanto sotto il profilo normativo e legale, ma soprattutto sotto il profilo tecnologico. In questo senso si sta procedendo alla elaborazione di tecniche che consentano l'elaborazione del *Sender Id*, il quale consentirebbe l'identificazione dello *spammer* eliminando uno dei trucchi maggiormente utilizzati, ovvero il c.d. *spoofing*, già

La proliferazione dello *spamming* provoca diversi problemi, in particolare: la perdita del tempo necessario per smaltire la posta indesiderata, i costi di connessione alla Rete occorrenti a scaricare sul computer messaggi anche molto pesanti, lo spazio occupato presso i server degli Internet Providers, la lesione della riservatezza a danno del ricevente la posta indesiderata¹¹, la possibilità, già verificatasi, che aziende e società commerciali o indirizzi istituzionali vengano fatti oggetto di veri e propri attacchi mirati degli *spammers*¹².

§2.1 La legislazione australiana: il Telecommunications Act 1997 e lo Spam Act 2003.

Ci si potrebbe domandare se sia possibile contrastare efficacemente il fenomeno dello *spamming* attraverso una strategia legislativa, oltre che con filtri software. A questo proposito, alcuni Stati si sono dotati di normative regolatrici del fenomeno¹³. Tra queste legislazioni vi è quella australiana, considerata una delle più moderne ed avanzate in tema di *spamming*. Già nel *Telecommunications Act 1997*¹⁴ è presente, contenuta nelle Section 112 e 113, una dichiarazione di intenti per la compilazione di previsioni regolatrici del comportamento delle imprese commerciali che utilizzino i servizi di telecomunicazione per i loro affari. In particolare, con il disposto della Section 112, il Parlamento federale ha inteso incaricare gli enti e le associazioni componenti l'ACMA (Australian Communications and Media Authority) di sviluppare codici di condotta

sanzionato penalmente negli Stati Uniti (E. O. Policella, *Op. cit.* p. 664; K. Greenstein, *Defending Your Brand From Email Spoofs*, in 784 *PLI/Pat* 271, 2004, p. 271; S. Austria, *Forgery In Cyberspace: The Spoof Could Be On You!*, in 5 *U. Pittsburgh J. Tech. L. & Pol'y* 2, 2002). La dottrina rileva che un'altra pratica da contrastare è *l'e-mail grabbing*, che consiste nella cattura materiale degli indirizzi di posta elettronica pubblici sul web (N. Lucchi, *Ult. Op. Loc. Cit.*).

¹⁰ *Australia Spam Report 2003*, cit.

¹¹ Il bene primario tutelato in relazione alle comunicazioni indesiderate è il diritto alla riservatezza dell'interessato. Esso va inteso nella sua accezione di "diritto di essere lasciati soli". Tale diritto è stato formulato dalla dottrina italiana sulla scorta del diritto anglosassone "*right to be alone*". Il concetto ha subito, peraltro, ulteriori evoluzioni come si evince dall'elaborazione del "diritto di essere lasciati in pace" (M. Atelli, *Chiamate indesiderate. Commento*, in AA. VV., *Privacy e telecomunicazioni. Commentario al D. Lgs. n.171/1998*, a cura di M. Atelli, Napoli, 1999, pag. 201) vi è poi chi si esprime in termini di "diritto alla tranquillità personale" (S. Vigliar, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Diritto dell'informazione e dell'informatica*, 2003, p. 419; M. A. Senior, *Comunicazioni indesiderate*, cit., p. 1 del manoscritto).

¹² S. I. Ahn, *Background Paper*, cit., p. 14; E. Hallace Kikuchi, *Spam In A Box: Amending Can-Spam & Aiming Toward A Global Solution*, 10 *B.U. J. Sci. & Tech. L.* 263 (2004), p. 268; E. Tosi, *La tutela dei dati personali*, in *I problemi giuridici di Internet*, (a cura di E. Tosi), Milano, 2003, p. 343; E. O. Policella, *Op. cit.*, p. 666; N. Lucchi, *Comunicazioni indesiderate*, cit., p. 457.

¹³ Recentemente anche la Nuova Zelanda ha approvato una specifica legislazione antispam, il *The Unsolicited Electronic Messages Bill 2005*", il quale fa esplicitamente riferimento al principio dell'*opt-in*. In dottrina, S. Harrison, *New Zealand: Legislation Against Spam*, in *Computer Law Review International*, 2005, p. 93.

¹⁴ La versione corrente, integrata con le previsioni dello *Spam Act 2003*, è stata emendata il 23 marzo 2006 ed è entrata in vigore lo stesso giorno. Consultata sul sito Internet il 1 aprile 2006 <http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/269D844D765651CDCA2571380081185B?OpenDocument>.

(*industry codes*) applicabili a coloro che operano nell'ambito delle attività di *e-marketing* delle attività concernenti la telecomunicazione. Nella successiva Section 113(3), il legislatore federale australiano ha specificato nel dettaglio quali siano i parametri di riferimento per la redazione dei suddetti codici. Essi riguardano le procedure a carico degli Internet Providers in materia di *spamming*, vale a dire il regolare uso, sviluppo e aggiornamento dei software che filtrano lo *spam*; la fornitura agli utenti di informazioni sulla disponibilità e sull'appropriato utilizzo dei medesimi, la minimizzazione e la prevenzione della spedizione o della consegna dei messaggi di *spam*, la chiusura dei server che inoltrino lo *spam*.

Lo *Spam Act 2003*¹⁵, approvato dal Parlamento Federale australiano il 18 settembre 2003 ed entrato in vigore il 10 aprile 2004, regola l'attività degli Internet Providers che utilizzino o spediscono, attraverso i loro server, messaggi pubblicitari a fini commerciali. La normativa presenta una serie di definizioni¹⁶ concernenti i messaggi elettronici¹⁷, il contenuto commerciale dei medesimi¹⁸, cosa si debba intendere per provenienza australiana¹⁹, l'autorizzazione alla

¹⁵ Il testo provvisorio dello *Spam Act 2003* è stato redatto da una "*Taskforce*" creata all'interno della *Internet Industry Association* che ha visto coinvolti direttamente i gestori di Internet Providers e altre parti interessate nel commercio elettronico. L'operazione è avvenuta nella più assoluta trasparenza attraverso la pubblicazione dei nomi dei membri della *Taskforce*, degli obiettivi del gruppo di lavoro e delle bozze del progetto su Internet, al sito web <http://www.ii.net.au/index.php>, consultato in data 1 aprile 2006. La *Taskforce* ha presentato una bozza dello *Spam Code* dove venivano recepite le linee guida indicate dal *Telecommunication Act 1997* e le indicazioni dell'ACMA (*Australian Communications and Media Authority*). Successivamente alla prima stesura, la bozza dello *Spam Act* è stata sottoposta al vaglio di altri enti istituzionali deputati al controllo della concorrenza, della trasparenza e della tutela dei consumatori quali l'ACCC (*Australian Competition and Consumer Commission*), il TIO (*Telecommunications Industry Ombudsman*), l'ACA (*Australia Consumers Association*), l'ISOC-AU (*Internet Society Australia*), il CAUBE (*Coalition Against Unsolicited Bulk Email*, Australia). La versione definitiva dello *Spam Act* è stata redatta tenendo conto del dibattito critico che le diverse voci hanno realizzato sulla bozza (*Internet Industry Spam Code of Practice, Explanatory Statement*, p. 4).

¹⁶ Per gli effetti dello *Spam Act 2003* sono messaggi elettronici quelli spediti usando un servizio di trasmissione via Internet collegato ad un account di posta elettronica, ovvero di *instant messaging*, o telefonico e simili, mentre viene esplicitamente esclusa la qualità di "messaggio elettronico" in capo alle chiamate vocali.

¹⁷ Il contenuto del messaggio elettronico può essere composto di dati, testo, immagini (statiche o in movimento), musica, suoni, anche in combinazione fra loro. (Sect. 6 *Commercial electronic messages*, *Spam Act 2003*).

¹⁸ Ai fini dello *Spam Act 2003*, sono considerati commerciali i messaggi aventi ad oggetto l'offerta di fornire beni e servizi, o la promozione pubblicitaria dei beni e servizi, del loro fornitore, di opportunità di conclusione di affari o finanziamenti, o il convincimento ottenuto con modalità dubbie rispetto alla buona fede al fine di conseguire un vantaggio di natura economico-patrimoniale a favore del mittente o di terzi (Sect. 6 *Commercial electronic messages*, *Spam Act 2003*).

¹⁹ Un messaggio elettronico commerciale è di provenienza australiana se, e solo se: il messaggio proviene dall'Australia, o coloro (persone fisiche, giuridiche, ovvero enti) che l'hanno spedito sono fisicamente presenti in Australia quando il messaggio è stato inviato, o la loro sede

spedizione dei messaggi da parte del ricevente²⁰ e l'applicazione territoriale delle sue disposizioni.

Le disposizioni dello *Spam Act 2003* proibiscono la spedizione, o la collaborazione alla spedizione, di "messaggi commerciali elettronici non sollecitati"²¹ provenienti da Internet Providers australiani²². Ne consegue che il consenso del destinatario alla ricezione di posta elettronica contenente messaggi commerciali deve essere espressamente manifestato secondo il principio comunemente conosciuto come "*opt-in*"²³. Tuttavia il divieto è meno restrittivo di quanto non appaia ad un primo sguardo, in quanto esso vieta l'invio di *spamming* solo se questo esso non sia un *designated commercial electronic message* e consista in un messaggio inviato da:

- un ente governativo (sia esso, un dipartimento, un'agenzia o un ente del Commonwealth, dello Stato Federale o del Territory, di un Paese straniero o di un ente governativo di un Paese straniero);
- un partito politico registrato (sia esso del Commonwealth, dello Stato federale o del Territory);
- una organizzazione religiosa, delle quali tuttavia lo *Spam Act 2003* non fornisce una definizione;
- una istituzione di carità, neanche questa definita nello *Spam Act 2003*;
- una istituzione con scopi educativi o formativi (cioè asili, scuole, college e università), se il destinatario è stato membro o studente di tali istituzioni formative.

In ogni caso i messaggi devono contenere precise informazioni sull'identificazione del mittente²⁴ e la funzione per la cancellazione del proprio indirizzo di posta elettronica dalla ricezione dei medesimi²⁵. Lo *Spam Act 2003* vieta altresì la raccolta²⁶ di indirizzi mail da fornire a individui, compagnie

centrale dei loro affari o del loro controllo è localizzata in Australia, come il computer, il server o il dispositivo che l'hanno inviato (Sect. 7 *Australian link*, *Spam Act 2003*).

²⁰ Sect. 8: *Authorising the sending of electronic messages*.

²¹ *Unsolicited commercial electronic message* (Sect. 16).

²² Il contrasto dello spamming è problematico a causa della difficoltà di bloccare i messaggi provenienti dall'estero. È stato calcolato che l'80% dello spam ricevuto dagli Internet Provider australiani proviene dagli Stati Uniti, mentre soltanto il 16% sarebbe di origine australiana (*NOIE Spam Final Report*, p. 10, consultato il 1 aprile 2006 sul sito Internet http://www.dcita.gov.au/__data/assets/pdf_file/21064/SPAMreport.pdf).

²³ M. E. Shames, *Congress Opt's Out Of Canning Spam*, in 66 *U. Pitt. L. Rev.* 385 (2004), p. 396.

²⁴ Section 17: *Commercial electronic messages must include accurate sender information*. Su questo punto lo *Spam Act* prevede che vengano pubblicate informazioni molto dettagliate: la chiara e accurata identificazione del mittente (si tratti sia di una persona fisica o giuridica), l'indicazione su come il ricevente possa contattare il mittente e che tale indicazione permanga valida ed accessibile almeno per i trenta giorni successivi all'invio della comunicazione.

²⁵ Section 18: *Commercial electronic messages must contain a functional unsubscribe facility*.

²⁶ Section 20, *Addresses – harvesting software and harvested – address lists must not be supplied*. Oggetto del divieto riguarda l'utilizzo di "*address-harvesting software or address-harvested list*", ovvero programmi software in grado di raccogliere indirizzi di posta elettronica setacciando la Rete.

commerciali ovvero *partnership* allo scopo di acquisto²⁷, ovvero uso²⁸, della mailing list così formata.

Le pene pecuniarie irrogate ai sensi dello *Spam Act 2003* sono calcolate in base alla reiterazione (sia nel numero, sia nel tempo) delle violazioni effettuate; mentre l'emanazione di *injunctions*²⁹ è collegata al riconoscimento di responsabilità civile a carico dello *spammer* qualora la vittima abbia sofferto perdite o danni in relazione alla lesione della reputazione, alla sua capacità di conclusione ovvero alla perdita di affari e in ogni altro caso che venga considerato rilevante dalla *Federal Court of Australia*³⁰.

La prima applicazione da parte della *Federal Court* della normativa *antispam* è avvenuta in occasione dell'azione proposta dall'ACMA contro la *Clarity1*, una società australiana accusata di aver violato le Sect. 16³¹ e 22³² dello *Spam Act 2003*. In concreto, la società è stata condannata per aver spedito almeno 56 milioni di messaggi commerciali indesiderati e di utilizzare *harvesting software* per formare *mailing list* da spammare³³. Justice Nicholson ha argomentato la decisione su due punti principali:

- a) che seppure i messaggi erano stati inviati con la possibilità del ricevente di dichiarare il proprio disinteresse al messaggio e far cancellare l'indirizzo dalla banca dati attraverso l'*opt-out*, lo *Spam Act 2003* considera valido e legalmente espresso soltanto il consenso preventivo alla ricezione dei messaggi commerciali elettronici secondo il principio dell'*opt-in*;
- b) sebbene prima della promulgazione dello *Spam Act 2003* non fosse vietato raccogliere *e-mail accounts* con *harvesting software*, dopo l'entrata in vigore del medesimo è illecito l'utilizzo di mailing list così formate.

Lo *Spam Act 2003* è stato oggetto di rilevanti critiche, specie da parte della *Electronic Frontiers Australia (EFA)*, l'associazione non governativa senza scopo di lucro che rappresenta la difesa delle libertà civili in Rete sul territorio australiano³⁴. Le critiche più consistenti riguardano l'effettività dell'applicazione dello *Spam Act 2003* in merito alla ricezione dei messaggi indesiderati e la vistosa presenza di diverse eccezioni all'applicazione dei divieti previsti dalla legge stessa, specie in merito ai messaggi inviati da enti caritatevoli, religiosi, partiti politici e istituzioni scolastiche, sia australiane, sia d'oltremare. Ulteriormente, un grande numero di emendamenti successivi alla sua promulgazione hanno reso oscura e di difficile applicazione la normativa.

²⁷ Section 21 *Address – harvesting software and harvested – address lists must not be acquired.*

²⁸ Section 22 *Address – harvesting software and harvested – address lists must not be.*

²⁹ Part 5, Sect. 31 – 36.

³⁰ Section. 40. *Assessment of compensation for breach of undertaking.*

³¹ Relativo alla spedizione di messaggi elettronici non sollecitati aventi contenuto commerciale.

³² Relativo all'utilizzo di software di raccolta di indirizzi mail nella rete (c.d. *harvesting software*).

³³ *Australian Communications and Media Authority v Clarity1 Pty Ltd [2006], FCA 410.*

³⁴ Rappresentanti e Statuto sono direttamente disponibili sul sito Internet dell'associazione <http://www.efa.org.au/AboutEFA/>

Le previsioni dello *Spam Act 2003* sono rimaste disattese per ciò che concerne le funzioni e le modalità di cancellazione dalla ricezione dei messaggi indesiderati perché la formulazione vaga del disposto legislativo ne rende di fatto inefficace la portata precettiva. La EFA sottolinea come nello *Spam Act 2003* manchino connessioni normative con le previsioni dei *Crimes Act 1914* e *Customs Act 1901* per quanto concerne l'aspetto della protezione della riservatezza e della violazione delle password e della crittografia.

Il 13 dicembre 2005 il Ministro Federale delle Comunicazioni, delle Arti e dell'Informatica ha convocato, fino al 1 febbraio 2006, una pubblica consultazione³⁵ avente lo scopo di raccogliere i contributi dell'opinione pubblica onde migliorare il testo dello *Spam Act 2003*. Il dibattito è stato focalizzato sulla precisazione delle previsioni normative di dubbia interpretazione, il contrasto dello *spamming* proveniente da oltremare, l'adeguamento delle previsioni con l'evoluzione delle tecnologie di comunicazione ed il coordinamento con l'intero *corpus* della legislazione australiana. Alla scadenza del termine previsto per la consegna dei contributi sono stati ricevuti 64 opinioni scritte di enti governativi, operatori commerciali, associazioni di consumatori, esperti e semplici cittadini. Questi contributi sono consultabili on line³⁶ e mentre altre tre opinioni sono state mantenute riservate. Entro il termine dell'anno in corso verrà reso pubblico il rapporto finale da sottoporre al Parlamento federale.

§2.2 Le nuove disposizioni dell'Internet Industry Spam Code of Practice.

In attuazione dello *Spam Act 2003*, la promozione pubblicitaria e il marketing effettuati per mezzo delle comunicazioni a distanza sono stati disciplinati con la promulgazione dell'*Australian eMarketing Code of Practices*³⁷ nel marzo 2005. L'*eMarketing Code* regola l'invio dei messaggi commerciali (emails, MMS, SMS, *instanting messages* ed in genere ogni messaggio commerciale inviato con mezzi di *Mobile Wireless Technology*) la cui ricezione sia stata espressamente autorizzata dal destinatario³⁸. Esso comprende disposizioni in merito al contenuto³⁹ e alla spedizione dei messaggi⁴⁰, alla registrazione⁴¹ e alla cancellazione⁴² del consenso manifestato dal ricevente e delle terze parti⁴³,

³⁵ Il bando è disponibile su Internet all'indirizzo web, consultato in data 10 aprile 2006, http://www.dcita.gov.au/__data/assets/pdf_file/34418/Spam_Review_Issues_Paper.pdf

³⁶ Press il sito web http://www.dcita.gov.au/ie/spam_home/spam_act_review2

³⁷ Previsto dalla *Section 109 A* del *Telecommunication Act 1997*, il quale definisce l'*eMarketing* come l'attività relativa all'invio di messaggi commerciali elettronici per la promozione di beni o servizi a destinatari che non siano fornitori professionali.

³⁸ Il testo è disponibile all'indirizzo Internet <http://www.acma.gov.au>.

³⁹ Rule 1. *Factual Communication*.

⁴⁰ Rule 2. *Sending Commercial Communication*; Rule 5. *Hours of Contact for MWT Commercial Communications*; Rule 6. *Viral Marketing and Member-Get-Member Schemes*.

⁴¹ Rule 3. *Record of Consent*; Rule 7. *Contact Information in Commercial Communications*; Rule 9. *Location Based Commercial Communications*.

⁴² Rule 10. *Functional Unsubscribe Facility*.

⁴³ Rule 4. *Third Part Contact*.

nonché relativamente all'accesso ai servizi a pagamento⁴⁴, alla tutela della privacy⁴⁵ e dei minori⁴⁶. Altresì è disciplinata la procedura di presentazione dei reclami degli utenti⁴⁷.

La *policy* australiana di regolamentazione e controllo della promozione pubblicitaria e dei messaggi commerciali, prevista dal *Telecommunication Act 1997*, vede aggiungersi ai già vigenti *Spam Code 2003* e *Australian eMarketing Code of Practice*, l'*Internet Industry Spam Code of Practice*. In questo modo l'utilizzo della Rete e delle comunicazioni a distanza per scopi commerciali è disciplinato in ogni suo spazio.

L'*Internet Industry Spam Code of Practice – A Code for Internet and Email Service Providers*⁴⁸ rappresenta una evoluzione ulteriore delle disposizioni del *Telecommunication Act 1997* e dello *Spam Act 2003* per ciò che concerne i messaggi indesiderati.

Il *Code* definisce precisamente che cosa è lo *spam*, cioè il messaggio commerciale elettronico che non sia sollecitato, che *non* includa informazioni accurate sull'identità del mittente e che non contenga le funzioni le quali consentono la cancellazione dell'indirizzo mail del ricevente⁴⁹.

Il nuovo codice comportamentale fonda la tattica di contrasto alla posta indesiderata con l'adozione di *Best Practices*⁵⁰ che impongano la previsione di tecniche *antispam* e i requisiti minimi che ciascun Internet Provider australiano⁵¹, compresi i servizi di *global mailing* quali *Hotmail* e *Yahoo!*, deve

⁴⁴ Rule 8. *Paid Subscription Services*.

⁴⁵ Nel *Foreword* l'*Australian eMarketing Code of Practices* fa espresso rinvio alle norme del *Privacy Act 1988*.

⁴⁶ Rule 11. *Sending Age-Sensitive Commercial Communications*.

⁴⁷ Rule 12. *Complaints Handling*.

⁴⁸ Il sottotitolo della normativa, disponibile al sito web <http://www.acma.gov.au/>, recita: "Co-Regulation in Matters Relating to Spam Email (consistent with the requirements of the Spam Act 2003 and Telecommunication Act 1997 to the extent it relates to the Spam Act). Alla Part. A, 1.1.4 viene espressamente previsto che in caso di conflitto tra l'*Internet Industry Spam Code of Practice*. – *A Code for Internet and Email Service Providers*, e la normativa precedente prevista dagli *Telecommunication Act 1997* e *Spam Code 2003*, vanno applicate le regole dell'*Internet Industry Spam Code of Practice*. L'*Internet Industry Spam Code of Practice* è stata promulgata il 27 marzo 2006 ed entrerà in vigour il 16 luglio 2006.

⁴⁹ Definizione contenuta nell'*Internet Industry Spam Code of Practice*, p. 12. Detta definizione fa esplicito riferimento alle Sections 16, 17 e 18 dello *Spam Act 2003*.

⁵⁰ Part. E, Sect. 9, in attuazione delle Sect. 109 e seguenti del *Telecommunication Act 1997* si intendono destinatari delle misure antispam i *Carriage Service Providers* e gli *Electronic messaging service providers* (Sect. 2 *Internet Industry Spam Code of Practice*).

⁵¹ Alla data della promulgazione del dell'*Internet Industry Spam Code of Practice*, risultano essere attivi in Australia ben 689 Internet Providers. Ai sensi delle Sect. 112(3) e 113 del *Telecommunication Act 1997* e della Part A dell'*Internet Industry Code*, ciascun Internet Provider deve registrarsi alla ACMA (Australian Communication and Media Authority) fornendo alcune informazioni relativamente al numero degli utenti finali che utilizzano i servizi dell'Internet Provider, quali attività dell'Internet Provider riguardano interessi commerciali e quali invece sono di pubblico interesse, oltre a specifiche informazioni sugli utenti finali (*Part. A, 1. Introduction and Registration with the ACMA, Internet Industry Spam Code of Practice*).

possedere. In tal senso il *Code*⁵² si propone un duplice obiettivo. Innanzitutto di bilanciare gli interessi dell'industria allo sviluppo dei metodi di *eMarketing*⁵³ responsabilizzando gli operatori nella minimizzazione dello *spamming*⁵⁴. Contestualmente, il raggiungimento nei consumatori⁵⁵ di una maggiore consapevolezza, cura e attenzione alla prevenzione dei pericoli cagionati dagli attacchi degli *spammers*. In siffatta prospettiva, gli Internet Providers australiani diventano i primi responsabili nella strategia di contrasto; essi hanno l'obbligo di:

- a) fornire agli abbonati⁵⁶ filtri *antispam*⁵⁷ e disporre di soluzioni alternative utilizzabili dagli utenti in caso di *default* dei filtri⁵⁸;
- b) informare gli utenti sull'attività di intercettazione della posta indesiderata e disporre delle regole contrattuali che proibiscano l'uso del *network* del Provider al fine impedire la diffusione dello *spamming*⁵⁹;
- c) collaborare con le preposte autorità investigative di contrasto allo *spamming*⁶⁰.

Oltre agli obblighi informativi⁶¹, il *Code* obbliga gli *Internet Service Providers* ad implementare alcune disposizioni. In dettaglio è previsto:

⁵² Dall'applicazione della disposizioni previste dal *Code* sono esclusi i messaggi inviati attraverso la modalità SMS e più in generale le norme in materia di E-Marketing contenute nell'*Australian e-Marketing code of Practice* (Sect. 2.1.4 dell'*Internet Industry Spam Code of Practice*).

⁵³ Part. A., Sect. 2.2.1. Il *Code* si propone anche altri obiettivi, che però si potrebbero definire programmatici e di lungo periodo, tra i quali: la riduzione della produzione e distribuzione dello Spam in Australia, l'incremento della trasparenza nella consegna dei messaggi di posta elettronica e l'incoraggiamento di un maggiore utilizzo di Internet da parte dei cittadini e delle imprese australiane.

⁵⁴ Part. A., Sect. 2.2.2.

⁵⁵ Il testo è stato scritto "in plain English" per assicurare che tutti gli utenti possano facilmente comprenderlo ed assimilarlo. Questo rilievo assume una sua importanza nell'ottica di assicurare le pari opportunità di accesso alle tecnologie informatiche contrastando la discriminazione tra aborigeni e popolazione di origine non indigena ancora molto presente nel Nuovissimo continente (J. Chesterman, B. Galligan, *Citizen without Rights. Aborigines and Australian Citizenship*, Cambridge, 1998; D. Mellor, *Contemporary Racism in Australia: The Experiences of Aborigines*, in *Personality And Social Psychology Bulletin*, 2003, IV, p. 474).

⁵⁶ Viene definito *subscriber*, abbonato, l'utilizzatore finale che abbia stabilito una relazione contrattuale con il Service Provider. Ciò parrebbe tutelare esclusivamente gli utilizzatori a pagamento dei servizi degli Internet Provider.

⁵⁷ In questo senso si è mossa l'ACMA medesima, rendendo disponibile per il download dal proprio sito il "*ACMA SpamMATTERS button*" in grado di intercettare lo spam, cancellarlo e redigere un report alla medesima autorità australiana sullo spam intercettato e cancellato. Potrebbero sorgere spontanee alcune perplessità sulla opportunità e liceità di un software di questo tipo: qualora il software cancellasse mail ritenute spam, mentre si tratta di importanti comunicazioni, chi risarcirebbe detta invasione della privacy? Software e FAC reperibili al sito web: http://www.acma.gov.au/ACMAINTER.65646:STANDARD:341044100:pc=PC_100097.

⁵⁸ Part. D, Sect. 6, *Spam Filters*.

⁵⁹ Part. F, Sect. 10, *Reporting Spam*.

⁶⁰ Part. C, Sect. 5. *Law Enforcement Issues*.

⁶¹ Part. B, Sect. 4, *Provision of Information*. Detti obblighi informativi riprendono le previsioni già affermate nel *Telecommunication Act 1997* e nello *Spam Act 2003*, ovvero che gli Internet Provider Service devono mettere gli abbonati in grado di attenersi alle disposizioni del *Code* e non porre

- d) il divieto della disponibilità a chiunque e senza controllo degli *open relay* o i *proxy server*. Gli Internet provider sono tenuti ad imporre ai propri utenti l'accettazione di questa esplicita clausola nelle *Acceptable Use Policies*⁶²;
- e) nel testo delle *Acceptable Use Policies* il diritto a favore degli Internet provider di scannerizzare e controllare i *networks* degli utenti non registrati e dei *proxy server*⁶³;
- f) assicurare, attraverso una previsione espressa nelle disposizioni delle *Acceptable Use Policies*, l'immediata disconnessione quando un *open relay server*, o un *open proxy server*, venga interessato in una infezione da virus o altra intrusione trasmessa involontariamente (per esempio attraverso un computer *zombie*)⁶⁴;
- g) nel caso in cui venga accertato che l'*account* di un utente sia diventato uno *spammer* (perché il suo computer si è trasformato in uno *zombie*, cioè un inconsapevole collettore di *spam*) l'*Internet Service Provider* deve mettere a disposizione dell'ignaro utente una apposita procedura onde avvertirlo e offrirgli assistenza per correggere il problema. È facoltà dell'*Internet Provider Service* interrompere la connessione con l'utente infetto qualora l'avaria sia grave e persistente⁶⁵;
- h) Gli *Internet Service Providers* possono memorizzare i dati registrati da indirizzi di *Internet Protocol* per un minimo di 7 giorni⁶⁶.

Per ciò che concerne le misure tecniche e le *best practices* contenute nel *Code*, esse possono riassumersi come segue. È consentita all'*Internet Service Provider*, o l'*E-mail Service Provider* la pubblicazione dei dossier inerenti all'attività dei filtri

in essere pratiche contrarie ad esso (4.1.a), informare gli utenti dell'esistenza del *Code* e dei suoi successivi cambiamenti (4.1. b e c), avvertire gli utenti sulle conseguenze del mancato rispetto delle norme di *Acceptable Use Policy* sulla produzione di spamming e predisposte dall'ISP in ottemperanza del *Code* (4.1.d), rendere disponibili suggerimenti e metodi onde ridurre al minimo la ricezione dello spam, utilizzare i filtri resi disponibili dagli ISP, segnalare all'ACMA i casi di ricezione di spam inerente a contenuti che possano offendere una persona adulta ragionevole (4.1.e), informare gli utenti che i messaggi ricevuti presso i loro account email vengono sottoposti obbligatoriamente alle procedure di filtro dello spam (4.1.f), e che questo potrebbe significare la perdita di messaggi non indesiderati (4.1.g). Va osservato come nel bilanciamento degli interessi venga privilegiato il contrasto allo *spamming* rispetto alla segretezza della corrispondenza e al diritto di ciascuno di ricevere la posta in entrata. La successiva section 4.2 obbliga la presenza del collegamento del ISP alle pagine web dell'ACMA relative allo spam ed obbliga anche agli IPS internazionali a predisporre procedure razionali alla lotta contro lo spamming.

⁶² Part. B, Sect. 4.2, *Provision of Information*.

⁶³ Part. E. Sect. 7, *Open Relays and Open Proxy*.

⁶⁴ Part. E. Sect. 7, *Open Relays and Open Proxy*.

⁶⁵ Part. E. Sect. 7, *Open Relays and Open Proxy*.

⁶⁶ Part E, Sect. 8, *IP Internet Address Information*. Questa ultima previsione può far sorgere fondati dubbi in merito alla tutela della riservatezza dei dati degli utenti degli Internet Service Providers australiani. In ogni caso è chiara la scelta di *policy* effettuata dall'ACMA, ovvero quella di sacrificare almeno in parte la riservatezza degli utenti in cambio di una maggiore efficacia nella lotta all'indiscriminata spedizione di messaggi indesiderati.

antispam da esso amministrati⁶⁷. Inoltre è previsto l'adeguamento dei parametri di sicurezza e affidabilità degli *Internet Service Providers* a quelli della APNIC⁶⁸ (*Asia Pacific Network Internet Center*)⁶⁹ e la collaborazione alla manutenzione dei dati di WHOIS in costante aggiornamento⁷⁰. L'*Internet Server Provider* può altresì limitare entro un ragionevole numero le E-mail che l'utente può spedire dal suo *account* di posta elettronica⁷¹, permettere agli utenti di autenticare le E-mail inviate attraverso un protocollo SMTP⁷², impedire la registrazione automatica di nuovi *E-mail account*⁷³, fornire modalità di accesso protette agli utenti che utilizzano i servizi Internet del Provider al fine di inviare messaggi di posta elettronica⁷⁴, infine, dove sia tecnicamente possibile e commercialmente sostenibile, inibire ai computer degli utenti di collegarsi ad indirizzi IP direttamente via *Port 25*⁷⁵.

Per ciò che concerne i reclami degli utenti finali sulla violazione delle previsioni del *Code*, e sulle relative sanzioni, esso rinvia alle disposizioni del *Telecommunication Act 1997*⁷⁶.

Leggendo i nomi dei componenti della *Spam Taskforce* che ha redatto il *Code*⁷⁷ è possibile fare alcune considerazioni relativamente all'impegno degli operatori professionali e commerciali nel contrasto delle comunicazioni indesiderate, consapevoli che un uso eccessivo e alterato dello strumento della

⁶⁷ Part E, Sect. 9, *Best Practices*.

⁶⁸ Part E, Sect. 9, *Best Practices*.

⁶⁹ L'*Asia Pacific Network Center* (APNIC), <http://www.apnic.net/index.html>, l'APNIC è uno dei cinque Registri Regionali di Internet esistenti al mondo. Si tratta di una organizzazione non governativa che funge da riferimento per la distribuzione degli indirizzi Internet e delle risorse ad esso collegate. L'APNIC è responsabile per gli *Internet Protocol* (IP) tra i parametri IPv4 e IPv6). Si occupa altresì di numeri identificativi degli *Autonomous System* (AS), e dei domini "in-addr.arpa".

⁷⁰ Attraverso i dati di WHOIS è possibile risalire al numero di *Internet Protocol* identificativo di ciascuno *Internet Service Provider*.

⁷¹ Part E, Sect. 9, *Best Practices*.

⁷² Part E, Sect. 9, *Best Practices*.

⁷³ Part E, Sect. 9, *Best Practices*.

⁷⁴ Part E, Sect. 9, *Best Practices*.

⁷⁵ Il "port 25" è la porta informatica che viene utilizzata da molti *Internet Service Providers* quale canale di comunicazione per spedire email tra l'*email account* del *client* e l'*email account* del server. Si tratta di uno dei canali privilegiati per l'attività di *spamming*, la creazione di filtri *antispam* in questo caso può portare a risultati deleteri, ovvero creare problemi agli e-mail servers e bloccare messaggi non indesiderati riconosciuti invece come spam. Il blocco di questo canale permette agli ISP di fermare la spedizione dello *spamming* attraverso i loro server. La soluzione alternativa sarebbe l'utilizzo di protocollo SMTP, già raccomandato dalle *best practices* contenute nel *Code*.

⁷⁶ Specificamente alla Part. 26, relative alle *Investigations*, ovvero dalla Sect. 507 alla Sect. 519. non essendo prevista una specifica Part relativa all'irrogazione delle violazioni e delle *injunction* per la violazione delle disposizioni del *Code*, è possibile sostenere che in materia vigano non solo le citate disposizioni del *Telecommunication Act 1997*, ma anche quelle dello *Spam Act 2003*, che calcolano l'importo della sanzione amministrativa a seconda del numero di volte in cui si è incorsi nella violazione.

⁷⁷ Pubblicati nella *Schedule 1, List of Contributors* in appendice all'*Internet Industry Spam Code of Practice*.

comunicazione elettronica provoca il fastidio dell'utente finale, vanificando lo scopo della comunicazione medesima.

§3. *Le disposizioni comunitarie in tema di spamming e di comunicazioni elettroniche non desiderate.*

Il diritto comunitario regola la disciplina delle comunicazioni elettroniche indesiderate sotto diversi aspetti:

- In *primis*, attraverso la tutela del diritto del consumatore ad una corretta, chiara e trasparente informazione nel commercio elettronico e nei contratti conclusi a distanza⁷⁸;
- Secondariamente, salvaguarda la tutela della riservatezza della vita privata e dei dati personali nella c.d. "società dell'informazione"⁷⁹;
- Infine, per mezzo delle disposizioni della recente direttiva 2005/29/CE sulle pratiche commerciali sleali⁸⁰.

L'art. 7 della Direttiva 2000/31/CE⁸¹, nota come direttiva sul commercio elettronico, ammette la liceità dell'invio di messaggi non sollecitati, a condizione che dai medesimi risulti chiaramente il carattere pubblicitario e che in precedenza all'invio i mittenti⁸² verifichino che i destinatari non si siano esplicitamente opposti alla ricezione, accogliendo a chiare lettere il principio dell'"opt-out"⁸³. L'art. 6 prevede che sia chiaramente identificabile la persona fisica o giuridica per conto della quale venga effettuata la comunicazione commerciale. Sempre la Direttiva 2000/31/CE, con il "Considerando" n. 14⁸⁴,

⁷⁸ P. Grugnola, *Disciplina dello spamming*, cit., p. 475; F. Di Ciommo, *Lo "spamming"*, cit., c. 2911.

⁷⁹ S. Vigliar, *Privacy e comunicazioni elettroniche*, cit., p.421; N. Lucchi, *Delle comunicazioni*, cit., p. 459; E. O. Policella, *Op. cit.*, p. 664.

⁸⁰ R. Incardona, *La direttiva sulle pratiche commerciali sleali: primi cenni*, in *Diritto comunitario e degli scambi internazionali*, n. 4, 2005, in pubblicazione, p. 2 del manoscritto, per gentile concessione dell'autrice.

⁸¹ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico"), pubblicata sulla Gazzetta Ufficiale delle Comunità Europee del 17 febbraio 2000 n. L. 178, e implementata nell'ordinamento italiano con il Decreto Legislativo 9 aprile 2003, n. 70 pubblicata sulla Gazzetta Ufficiale del 14 aprile 2003 Supplemento Ordinario n. 61.

⁸² Attraverso la creazione di "registri negativi", o di liste di opposizione, previsti dalla stessa direttiva 31/2000/CE. Sul punto, S. Vigliar, *"Privacy e comunicazioni"*, cit., p. 421; E. O. Policella, *Op. Cit.*, p. 665).

⁸³ Il concetto di "opt-out", relativo all'esplicito rifiuto del destinatario di ricevere comunicazioni commerciali, è stato introdotto dalla direttiva 97/7/CE, inerente alla protezione dei consumatori nei contratti conclusi a distanza (S. Vigliar, *Ult. Op. Loc. Cit.*; O. E. Policella, *Ult. Op. Loc. Cit.*).

⁸⁴ Per comodità del lettore se ne propone di seguito il testo "(14) La protezione dei singoli relativamente al trattamento dei dati personali è disciplinata unicamente dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e dalla direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle

offre la chiave di lettura per comprendere la diversità delle impostazioni delle strategie di *policy* in tema di tutela della privacy, protezione del consumatore e contrasto alla proliferazione dello *spamming* tra Europa e Australia. Il "Considerando" 14 dichiara infatti che "la presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet". Al contrario è ciò che il Parlamento federale australiano, attraverso organi istituzionali quali l'ACMA, tenta di impedire, almeno per quanto concerne il territorio nazionale, con l'aggravio di responsabilità a carico degli *Internet Service Providers*, come si è visto poco sopra.

La tematica della tutela della riservatezza contro l'invasione delle comunicazioni indesiderate è stata affrontata già nelle direttive CE/46/1995⁸⁵ e CE/66/1997⁸⁶, ma è con la direttiva CE/58/2002⁸⁷, la quale integra e sostituisce le precedenti⁸⁸, che viene introdotto un divieto espresso di *spamming* destinato ai privati cittadini. Esso è previsto nel testo dell'art. 13 della Direttiva, la quale prevede sia l'accoglimento del principio di "opt-in"⁸⁹, sia il divieto dell'utilizzo

telecomunicazioni, che sono integralmente applicabili ai servizi della società dell'informazione. Dette direttive già istituiscono un quadro giuridico comunitario nel campo della protezione dei dati personali e pertanto non è necessario includere tale aspetto nella presente direttiva per assicurare il buon funzionamento del mercato interno, in particolare la libera circolazione dei dati personali tra gli Stati membri. L'applicazione della presente direttiva deve essere pienamente conforme ai principi relativi alla protezione dei dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari. La presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet".

⁸⁵ Direttiva 1995/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pubblicata sulla Gazzetta Ufficiale delle Comunità Europee del 23 novembre 1995, n. 281 e recepita nell'ordinamento italiano con la legge del 31 dicembre 1996, n. 675, pubblicata nella *Gazzetta Ufficiale* n. 5 dell'8 gennaio 1997 - Supplemento Ordinario n. 3.

⁸⁶ Direttiva 66/1997/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, pubblicata sulla Gazzetta delle Comunità Europee del 30 gennaio 1998, n. 24 e recepita nell'ordinamento italiano con il D. Lgs. 13 maggio 1998, n. 171, pubblicato sulla Gazzetta Ufficiale del 3 giugno 1998, n. 127.

⁸⁷ 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 (Direttiva relativa alla vita privata e alle comunicazioni elettroniche), pubblicata nella Gazzetta Ufficiale delle Comunità Europee n. 201 del 31 luglio 2002 e recepita nell'ordinamento italiano con il D. Lgs 30 giugno 2003, n.196, "Codice in materia di protezione dei dati personali" e pubblicato sulla Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

⁸⁸ N. Lucchi, *Op. cit.*, p. 459.

⁸⁹ Ovvero che l'invio di comunicazioni commerciali o pubblicitarie è legittimo esclusivamente in presenza del previo consenso del destinatario (F. Di Ciommo, *Op. cit.*, c. 2908; A. Sica, *Commento agli artt. 121 – 132*, in *La nuova disciplina della privacy. Commento al d. lgs. 30 giugno 2003, n. 196*, (a cura di S. Sica e P. Stanzone), Bologna, 2005, p. 585). Infatti, il testo del c. 1 dell'art. 13 della Direttiva CE/58/2002 afferma che: "1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta

delle tecniche di *spoofing* da parte del mittente delle comunicazioni indesiderate, cioè camuffando o celando la propria identità o riferimenti ad essa⁹⁰. Va evidenziato che il terzo comma dell'art. 13 lascia agli Stati membri, in sede di attuazione della normativa comunitaria, la libertà di scelta tra il regime di *opt-in* e *opt-out*⁹¹ per vietare l'invio delle comunicazioni indesiderate a scopo di commercializzazione diretta⁹². Va evidenziato che l'esplicito riferimento alla "commercializzazione diretta" esclude dall'applicazione della direttiva gran parte dello *spamming* avente contenuto messaggi di altra natura, per esempio contenuti religiosi, ideologici, politici e così via⁹³.

La dottrina non è concorde sulla efficacia di tali disposizioni. Vi è chi osserva che in ogni caso la Direttiva 2000/58/CE offre una libertà di scelta che non è soddisfacente né sotto il profilo della tutela della privacy e né per ciò che concerne le problematiche relative all'applicabilità della norma medesima, considerato che il mercato offerto da Internet è transnazionale⁹⁴. Ciò comporterebbe due tipi di problemi. Il primo riguarderebbe gli operatori che praticino la commercializzazione diretta negli Stati membri in cui esiste il sistema del consenso preventivo esplicito (*opt-in*): se da un lato costoro non possono inviare messaggi elettronici a destinatari che risiedono nel loro Paese, possono continuare ad inviare messaggi non sollecitati dove vige il sistema della revoca del consenso (*opt-out*), ponendo comunque in essere un comportamento illecito. Il secondo problema concernerebbe il fatto che gli indirizzi di posta elettronica possono non contenere indicazione relativamente alla residenza dei destinatari, e ciò rende vana la distinzione tra *opt-in* e *opt-out* effettuata al momento della implementazione della normativa comunitaria nell'ordinamento nazionale.

Per quanto concerne gli orientamenti comunitari in tema di protezione dallo *spamming*, recentemente i Garanti europei della Privacy hanno sottoscritto un documento dove viene concesso al provider l'autorizzazione ad effettuare la scansione automatizzata della posta elettronica alla ricerca di virus o di *spam*

elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso".

⁹⁰ Afferma il testo dell'art. 13, c.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".

⁹¹ M. Maglio, *Scusi, ma lei è "optinista" o "optautista"?*, consultato sul sito Internet www.interlex.it in data 10 aprile 2006. Sul tema va segnalata la Raccomandazione n. R (85) 20 sulla protezione dei dati personali usati per finalità di *marketing* diretto adottata dal Consiglio d'Europa il 25.10.1985, riportata e tradotta in *Dir. inf. inf.*, 1986, p. 992.

⁹² S. Vigliar, *Op. cit.*, p. 422. Si propone il testo del citato 3° comma dell'art. 13 della direttiva CE/58/2002: "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".

⁹³ S. Vigliar, *Op. cit.*, p. 423.

⁹⁴ S. Vigliar, *Op. cit.* p. 422; P. Crugnola, *Op. cit.*, p. 479.

senza il consenso dell'utente o dell'abbonato. In ogni caso il Provider è obbligato a richiedere detto consenso qualora lo scopo dello *screening* delle e-mails sia di individuare contenuti potenzialmente illegali (quali i *files* a carattere pornografico o a contenuto razzista)⁹⁵. Al riguardo affermano i Garanti europei della Privacy che si tratta di operazioni di scansione lecite purché rientranti negli obblighi di sicurezza posti dalla direttiva 2002/58/CE e delle norme nazionali di implementazione. Questa attività non richiede il consenso preventivo dell'utente, ma non esime il provider dai suoi obblighi di adeguata informazione sulla natura della prestazione, di non rivelazione del contenuto dei messaggi e di limitazione alla ricerca di possibili virus quando la scansione venga effettuata anche sul contenuto dei medesimi⁹⁶.

Attenta dottrina osserva che è possibile individuare una estensione della tutela delle parti commercialmente deboli per quanto ha attinenza con il leale svolgimento delle pratiche commerciali delle imprese che incidono sugli interessi economici dei consumatori⁹⁷, ai sensi della direttiva 2005/29/CE⁹⁸. La lista nera delle pratiche commerciali ingannevoli, prevista dall'allegato I della Direttiva, include tra i comportamenti sleali l'"effettuare ripetute e sgradite sollecitazioni commerciali per telefono, via fax, per posta elettronica o mediante altro mezzo di comunicazione a distanza, fuorché nelle circostanze e nella misura in cui siano giustificate dalla legge nazionale ai fini dell'esecuzione di un'obbligazione contrattuale". Va osservato, tuttavia, che la norma si riferisce genericamente alla "natura" della pratica commerciale, e non anche al "mezzo" utilizzato. Anche in assenza di richiamo allo *spamming*, viene fatto un riferimento esplicito alla posta elettronica. Di conseguenza è possibile fondatamente ritenere che l'invio seriale di E-mail non consentite ed aventi

⁹⁵ Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, consultato in data 7 aprile 2006 sul sito Internet http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf.

⁹⁶ Newsletter del Garante della Privacy del 7 marzo 2002 n. 272, consultata in data 7 aprile 2006 sul sito Internet www.garanteprivacy.it. In merito alla scansione dello spam, il Garante precisa che: "Anche lo screening effettuato per individuare spam è, a giudizio dei Garanti Ue, attività assimilabile all'attivazione di misure di sicurezza, poiché lo spam compromette la funzionalità dei servizi di posta elettronica. Tuttavia, in considerazione del rischio di generare "falsi positivi" - ossia di filtrare come spam messaggi che in effetti non lo sono - e dunque di limitare in qualche misura la libertà di comunicazione, i provider dovrebbero consentire agli utenti di disapplicare i filtri anti-spam e di stabilire quali tipi di spam debbano essere filtrati. In particolare, il Gruppo di lavoro invita i provider e i produttori di software e programmi di posta elettronica a mettere a punto strumenti che diano all'utente la possibilità di configurare autonomamente i meccanismi di filtraggio anti-spam."

⁹⁷ R. Incardona, *Op. cit.*

⁹⁸ Direttiva 2005/29/CE del Parlamento Europeo e del Consiglio dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali»), pubblicata sulla Gazzetta Ufficiale delle Comunità Europee dell'11 giugno 2005 n. 149/22.

contenuto commerciale configuri una pratica commerciale sleale⁹⁹, sottoposta alla direttiva CE/29/2005.

La comparazione tra diritto comunitario e normativa australiana sollecita alcune riflessioni. La normativa comunitaria mantiene una certa neutralità rispetto alla tecnologia utilizzata, in quanto il processo di convergenza tra le tecnologie attualmente in atto consente di allargare il medesimo servizio mediante l'utilizzo di tecnologie differenti ed in continua evoluzione. Le scelte europee, quindi sono orientate a considerare che una regolamentazione strettamente settoriale può divenire obsoleta nel breve periodo o comportare distorsioni del mercato orientando gli investimenti dei produttori¹⁰⁰. All'opposto, l'*Internet Industry Spam Code of Practice* si occupa nel dettaglio di regolare dal punto di vista giuridico le procedure e i protocolli tecnico-informatici e lascia scarsa possibilità di scelta agli Internet Service Providers, essendo questi vincolati ad una serie di *Best Practices* già largamente predeterminate nel contenuto dall'*Australian Communication & Media Authority*. Tali differenze sono maggiormente evidenti in merito a caratterizzanti scelte di *policy*, qualora si consideri la fonte normativa che ha emanato la regolamentazione *antispam*. Nel caso australiano si tratta di una *Autorithy* Federale indipendente, mentre la normativa comunitaria deve rispettare i requisiti previsti dai Trattati Comunitari sacrificando, in virtù del principio di sussidiarietà, una maggiore incisività nella scelta di una strategia comune.

§4.1 Il quadro normativo italiano.

Nell'ordinamento italiano, le comunicazioni commerciali indesiderate sono regolamentate dall'art.130 del Codice della Privacy, il quale dispone che "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"¹⁰¹. L'art. 130 del Codice della privacy ratifica

⁹⁹ R. Incardona, *Op. cit.*, e dottrina ivi suggerita in tema di *Internet* e le pratiche commerciali sleali in generale vedasi S. Peron, *Concorrenza sleale on-line: rassegna di giurisprudenza*, in *Riv. dir. ind.*, 2002, p. 73; C. Asprella, *Brevi cenni su Internet, concorrenza sleale e giudice competente per territorio*, in *Giur. Merito*, 2001, p. 916; G. Bonomo, *Il nome di dominio e la relativa tutela. Tipologia delle pratiche confusorie in internet*, in *Riv. dir. ind.*, 2001, p. 247; F. Sebastio, *Libera concorrenza, pubblicità e concorrenza sleale, decettività del marchio*, in *Giust. civ.*, 1999, p. 703; L. Albertini, *Le comunicazioni via Internet di fronte ai giudici: concorrenza sleale ed equiparabilità alle pubblicazioni a stampa*, in *Giust. civ.*, 1998, 1, p. 259.

¹⁰⁰ S. Vigliar, *Op. cit.*, p. 402.

¹⁰¹ Il secondo comma della disposizione prevede che: "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". Sul tema, il Garante della privacy ha più volte affermato che il consenso manifestato dal titolare dei dati personali (in questo caso dell'indirizzo di posta elettronica) deve essere manifestato in modo "specifico e informato" (Garante della Privacy, 11 ottobre 2001, in *Cittadini e società dell'informazione*, 2001, p. 39; Id., 7 giugno 2004, *ivi*, 2004, doc. web. N. 1040958; Id., 16 giugno 2004, in *ivi*, 2004, doc. web., N. 1041161), altre volte ha operato il blocco i data base di altre sette società che operano in Internet per aver violato le norme sulla

nell'ordinamento italiano l'art. 13 della Direttiva CE/58/2002, adeguandosi all'accoglimento del principio dell'*opt-in*, ovvero del previo consenso del destinatario. Il 5° comma dell'art.130 contempla il divieto di altre comunicazioni indesiderate limitandosi a indicare esclusivamente quelle commerciali o promozionali che vengano inviate attraverso lo *spoofing*.

Nel Codice della privacy, che recepisce la direttiva 2000/58/CE, è stato mantenuto l'esplicito riferimento ai "messaggi commerciali indesiderati" o inerenti alla "vendita diretta". Detto richiamo espresso esclude dall'applicazione della tutela della privacy e delle sanzioni da essa previste la grande maggioranza dei messaggi di *spamming*. Tale limite è difficilmente superabile, se non in sede di redazione dei codici deontologici previsti dagli articoli 133 e 140 del Codice medesimo e allo stato ancora non approvati per tutte le categorie professionali interessate al trattamento dei dati personali degli utenti¹⁰².

La lotta allo *spamming* è stata oggetto dell'emanazione di un provvedimento generale dell'Autorità Garante della protezione dei dati personali¹⁰³. Nel testo, il Garante ha ribadito alcuni obblighi per i providers, ovvero:

- a) che gli indirizzi di posta elettronica contengono dati di carattere personale da trattare ai sensi della normativa in materia;
- b) che la loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato, ribadendo in questo modo il

privacy. Dette società avevano inviato varie e-mail pubblicitarie e promozionali senza aver acquisito il consenso dei destinatari prima di inviare i messaggi commerciali e senza fornire le prescritte informazioni su modalità e finalità della raccolta dei dati personali (Newsletter del Garante della privacy 24-30 marzo 2003, n. 164).

¹⁰²In combinato disposto con l'art. 12, co. 3 del Codice della Privacy. L'emanazione dei codici deontologici e di buona condotta era già prevista dall'art. 20 del D. Lgs. 467/2001. L'unico codice deontologico approvato successivamente a questa normativa riguarda il "Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti", pubblicato sulla G. U n. 300 del 24 dicembre 2004. Mentre gli altri codici deontologici attualmente in vigore, anche promulgati anteriormente al codice della Privacy, sono "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale", pubblicato nella Gazzetta Ufficiale del 1 ottobre 2002, n. 230, il "Codici di deontologia e di buona condotta relativi ai trattamenti di dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica; necessari per finalita' previdenziali o per la gestione del rapporto di lavoro; effettuati a fini di invio di materiale pubblicitario; a fini di informazione commerciale; nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo; provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici; effettuati con strumenti automatizzati di rilevazione di immagini" pubblicato sulla Gazzetta Ufficiale dell'8 maggio 2002, n. 106 e il "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici", pubblicato sulla Gazzetta Ufficiale del 5 aprile 2001, n. 80. In dottrina, E. O. Policella, *Op. cit.*, p. 666.

¹⁰³ Emanato il 29 maggio 2003 ed consultato in data 10 aprile 2006 sul sito Internet www.garanteprivacy.it. In dottrina, A. Sica, *Op. cit.*, p. 585; E. O. Policella, *Op. cit.*, p. 666.

principio dell'*opt-in*¹⁰⁴. Analogo consenso è necessario "anche quando gli indirizzi sono formati ed utilizzati automaticamente con un software senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi";

- c) vietando l'utilizzo degli *Addresses – harvesting software*, ovvero della raccolta attraverso programmi software (o manualmente) di indirizzi di posta elettronica reperibili su Internet, considerato "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";
- d) che il silenzio dell'utente non può essere considerato una forma di consenso al trattamento, ma che in ogni caso debba essere interpretato quale diniego al medesimo.

Il provvedimento del Garante statuisce come l'accertato trattamento illecito dei dati personali comporti il rimborso delle spese legali e il riconoscimento dei diritti relativi all'azione dinanzi al giudice civile. In particolare, il risarcimento del danno patrimoniale riconducibile all'invio dello *spamming* non autorizzato. Gli aspetti concreti rilevanti del danno sono collegati al tempo occorso per selezionare i messaggi da cancellare perché indesiderati e il pagamento dei maggiori costi di connessione¹⁰⁵.

Il quadro così delineato potrebbe essere modificato dalla recente legge di promulgazione del decreto c.d. "Milleproroghe"¹⁰⁶. In dottrina ci si domanda se tale innovazione legislativa abbia avuto effetti modificativi sia sulla recente consolidazione della normativa consumeristica¹⁰⁷, sia sulle disposizioni del

¹⁰⁴ Principio ribadito con il Provvedimento dell'Autorità Garante della Privacy emesso in data 20 aprile 2006 (doc. web n. 1289884), e comunicato al pubblico con la newsletter del 29 maggio 2006 disponibile sul sito www.garanteprivacy.it. Nella fattispecie in esame, nonostante la società mittente della mail commerciale indesiderata si sia giustificata spiegando che quel primo invio era volto solo a richiedere il consenso per il successivo inoltro di comunicazioni commerciali, l'Autorità ha confermato il netto rifiuto della prassi di mandare una mail pubblicitaria senza consenso e poi scusarsi affermando che comunque quella era l'unica comunicazione inviata. Nella sua decisione l'Autorità ha spiegato che occorre ottenere sempre il consenso del destinatario prima di effettuare qualunque uso dell'indirizzo di posta elettronica se l'invio è a fini di pubblicità e marketing. Ripetendo un principio fondamentale per l'uso degli indirizzi e-mail, l'Autorità ha poi sottolineato che un indirizzo di posta elettronica per il solo fatto di essere sia reperibile in rete non autorizza comunque un suo uso indiscriminato.

¹⁰⁵ Provvedimento del Garante cit.; E. O. Policella, *Op. cit.*, p.667; N. Lucchi, *Op. cit.*, p. 462; E. Florindi, *Spam e tutela della riservatezza*, cit. p. 184.

¹⁰⁶ Legge 23 febbraio 2006, n.51 "Conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273, recante definizione e proroga di termini, nonché conseguenti disposizioni urgenti. Proroga di termini relativi all'esercizio di deleghe legislative" pubblicata sulla Gazzetta Ufficiale n. 49 del 28 febbraio 2006, Suppl. Ordinario n. 47).

¹⁰⁷ Effettuata con il D. Lgs. 6 settembre 2005, "n. 206, "Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229", pubblicato nella Gazzetta Ufficiale n. 235 del 8 ottobre 2005 - Supplemento Ordinario n. 162.

Codice della Privacy. Nel testo della legge 23 febbraio 2006, n. 51 va evidenziata la presenza di un precetto normativo che potrebbe avere effetti rilevanti sull'intero impianto legislativo in tema di consenso informato e di comunicazioni commerciali indesiderate. L'art.19 bis così recita: "deroga al d.lgs. 196/03 - l'art. 58 comma 2 del codice del consumo¹⁰⁸ di cui al d.lgs. 206/05, si applica anche in deroga alle norme di cui al d.lgs. 196/03". Gli effetti pratici di questa nuova disposizione riguardano la scelta di *opt-in* (prevista dal primo comma dell'art. 58 del D. Lgs. 206/2005) ovvero di *opt-out* (previsto dal secondo comma del medesimo decreto). Il nuovo disposto normativo vigente dopo l'entrata in vigore della legge 51/2006 apparentemente accorderebbe l'invio di messaggi indesiderati senza il consenso del destinatario, ribaltando sul ricevente l'onere di pretendere la cancellazione del proprio mail account dalle banche dati del mittente. La dottrina¹⁰⁹ pone in evidenza due rilievi di natura sistematica cui tale novità legislativa sarebbe affetta. Innanzi tutto si tratterebbe di una normativa costituzionalmente viziata, in quanto l'art. 19 -bis è stato inserito nella legge di conversione del decreto legge "Milleproroghe", ma non era contemplata nel decreto legge convertito. Il secondo rilievo concerne il fatto che l'art. 58, 2° comma del Codice del consumo si riferisce esclusivamente alle tecniche di comunicazione a distanza che non siano quelle inserite nel primo comma (ovvero telefono, posta elettronica, sistemi automatizzati di chiamata e fax). In conseguenza di ciò l'ambito di applicazione dell'esenzione del consenso preventivo sarebbe estremamente contenuto¹¹⁰. Ciononostante è da sottolineare la mancanza di una strategia coerente e univoca in tema di spedizione elettronica di comunicazioni commerciali da parte del legislatore italiano.

§4.2. Le responsabilità degli Internet Service Providers Italiani.

Nell'ordinamento italiano non sono contemplate previsioni specifiche per coloro che concretamente pongano in essere attività di *spamming*. Onde sanzionare la spedizione elettronica di messaggi commerciali non richiesti è necessario fare riferimento alle disposizioni previste per la tutela della riservatezza dei dati personali, quale è l'indirizzo e-mail del destinatario.

Per ciò che riguarda l'aspetto penalistico, l'inosservanza delle disposizioni dell'art. 130 del Codice della Privacy, cioè la mancata raccolta del consenso all'utilizzo dell'indirizzo di posta elettronica per l'invio di messaggi

¹⁰⁸ Il testo dell'art. 58 del D. Lgs. 206/2006 recita: (Limiti all'impiego di talune tecniche di comunicazione a distanza), 1. L'impiego da parte di un professionista 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 professionista se il consumatore non si dichiara esplicitamente contrario.

¹⁰⁹ P. Ricchiuto, *Privacy e comunicazioni indesiderate: un nuovo capitolo*, in www.interlex.it consultato in data 10 aprile 2006

¹¹⁰ P. Ricchiuto, *Privacy e comunicazioni indesiderate*, cit.

commerciali o promozionali, espone il titolare del trattamento alla sanzione penale di cui all'art.167 del medesimo codice¹¹¹. Tale articolo delinea il reato di illecito trattamento dei dati personali punito con la reclusione da sei a diciotto mesi. Affinché vi sia la completa integrazione della fattispecie di reato, insieme alle circostanze previste dall'art.130 del Codice della privacy, occorre anche la finalità di trarre un profitto o di arrecare ad altri un danno, l'esistenza di un documento¹¹². Congiuntamente, l'esecuzione di un'attività di *spamming*, senza la preventiva informazione del soggetto interessato, espone alla sanzione amministrativa di omessa informativa, ai sensi dell'art. 161 del Codice della Privacy, la quale ammonta da tremila a diciottomila Euro¹¹³.

Sotto il profilo civilistico, il trattamento dei dati personali viene equiparato dal legislatore all'esercizio di un'attività pericolosa, ai sensi dell'espresso richiamo dell'art. 2050 c.c. contenuto nell'art.15 del Codice della privacy¹¹⁴. La giurisprudenza ha illustrato in che cosa consista il concetto di "pericolosità", ovvero nella rilevante possibilità del verificarsi del danno per l'elevata potenzialità offensiva dell'attività intrapresa¹¹⁵. In mancanza di tale richiamo espresso alla responsabilità civile per attività pericolose, sarebbe stato difficile che la giurisprudenza potesse modificare il suo consolidato orientamento che riconosce l'applicabilità dell'art. 2050.c.c. esclusivamente alle ipotesi di danno all'integrità fisica¹¹⁶. In dottrina, tuttavia, le voci non sono unanimi. Vi è chi

¹¹¹ F. Di Ciommo, *Op. cit.*, c. 2911; D. D'Agostini, *Op. cit.*, p. 226.

¹¹² Afferma la Cassazione: "La modifica più evidente apportata dal D.Lgs 196/03 all'articolo 35 legge cit. ora articolo 167 consiste sul piano strutturale nella previsione nella fattispecie criminosa base dell'elemento del "documento" attraverso la locuzione «se dal fatto deriva documento», precedentemente costituente soltanto una circostanza aggravante, sicché il delitto è stato trasformato da reato di pericolo presunto a quello di pericolo concreto con un'ulteriore maggiore tipicizzazione del danno e del profitto" (Cass. pen., 28 maggio – 9 luglio 2004, n. 30134, Pres. Savignano, Est. Novarese, pubblicata su www.interlex.it; in dottrina, E. O. Policella, *Op. Cit.*, p. 667). La giurisprudenza di merito ha affermato che il documento non sia configurabile *in re ipsa* come nel caso dell'invio di "un solo messaggio non ripetuto che non ha provocato un concreto vulnus alla persona offesa, ma una lesione minima della privacy che non ha determinato un danno patrimonialmente apprezzabile" (Gup Udine, dott. Scaramuzza, 6 maggio 2005, disponibile su www.altalex.it).

¹¹³ In caso di mancato rilascio dell'informativa in presenza di un trattamento di dati sensibili o giudiziari, la sanzione da comminare va da cinquemila a trentamila euro. Tale sanzione può essere comminata direttamente da parte del Garante per la protezione dei dati personali e può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore (E.O. Policella, *Ult. op. loc. cit.*).

¹¹⁴ In dottrina, a proposito della qualificazione giuridica della forma di responsabilità prevista dall'art.2050, non vi è un orientamento uniforme, considerato che la responsabilità civile per attività pericolosa viene considerata da alcuni come una forma di colpa presunta e da altri come una forma di responsabilità speciale aggravata (E. O. Policella, *Op. cit.*, p.668).

¹¹⁵ Cass., 23 febbraio 1983, n. 1384; Cass., 21 dicembre 1992, n. 13530, in *Resp. Civ. e Prev.*, 1993, p. 821; Cass., 27 luglio 1990, n. 7571, in *Arch. Civ.*, 1991, p. 46.

¹¹⁶ Tale orientamento ha resistito alle forti critiche poste da autorevole dottrina in tema di estensione dell'ambito delle attività pericolose alle ipotesi di gestione delle banche dati (G. Alpa, *Computers e responsabilità civile*, Milano, 1985; P. Morozzo della Rocca, *Gestione di banche*

ritiene che non possa essere accolta l'equiparazione dell'attività di raccolta dei dati ad attività pericolosa in quanto sorgerebbero diversi problemi di ordine pratico¹¹⁷.

Sotto l'aspetto della ripartizione dell'onere probatorio tra attore (il soggetto danneggiato e titolare dei dati personali illecitamente trattati) e il convenuto (il soggetto danneggiante e titolare del trattamento) va sottolineato che ci subisce il danno in conseguenza dell'illecito trattamento dei dati personali è tenuto a fornire la prova dell'esistenza del danno nonché del nesso di causalità tra l'attività illecita e il danno cagionato¹¹⁸. In questo senso, la giurisprudenza di merito ha chiarito che il richiamo all'art. 2050 c.c. non comporta l'inversione dell'onere probatorio¹¹⁹. In dottrina vi è chi sostiene che il destinatario dello *spamming* può limitarsi a provare di aver subito un danno a causa dell'invio di comunicazioni indesiderate¹²⁰.

Per quanto concerne la quantificazione del danno la scarsa giurisprudenza sul punto si è divisa. Da un lato si sostiene che l'invio di posta elettronica indesiderata costituisce un fatto illecito produttivo di responsabilità civile sia per la scorrettezza e l'illiceità del trattamento del titolare dell'indirizzo bersaglio, sia per l'invasione della sfera di riservatezza del medesimo¹²¹; mentre dall'altro si afferma che l'invio di un singolo messaggio indesiderato di posta elettronica non lede il diritto della privacy e conseguentemente non dà luogo a responsabilità civile in capo al mittente¹²².

dati e problemi della responsabilità civile, in *Legalità e giustizia*, 1988, p. 326, E. O. Policella, *Ult. op. loc. cit.*).

¹¹⁷ Tale dottrina sostiene che il rinvio all'art. 2050 c.c. è da considerarsi parziale perché esso indicherebbe "le regole per l'esonero della responsabilità mentre nel complesso normativo del Codice debbono essere individuate le indicazioni relative alla identificazione dell'autore, alla antigiusuridicità della condotta, alla determinazione del danno risarcibile ed ai criteri quantificatori del danno (D. Simboli, *Il diritto alla protezione dei dati personali*, (a cura di R. Acciai), Rimini, 2004, p. 327).

¹¹⁸ F. Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile*, 2003, p. 315.

¹¹⁹ Trib. Milano, 8 agosto 2003, in *Danno e resp.*, 2004, p. 303; Trib. Biella, 26-29 marzo 2003, in *Guida dir.*, n.15, p. 70; Trib. Napoli, 3 febbraio 2003, in *Giur. nap.*2003, p. 191; Trib. Orvieto, 25 novembre 2002, in *Danno e resp.*, 2003, p. 281.

¹²⁰ D. D'Agostini, *Op. cit.*, p. 227.

¹²¹ Giudice di Pace di Napoli, 10 giugno 2004, in *Foro it.*, 2004, c. 2908, con nota di Di Ciommo; *Danno e resp.*, 2005, p. 659, con nota di E. O. Policella. Nello stesso senso vanno inquadrare le pronunce relative alla ricezione indesiderata di SMS di propaganda sia commerciale sia elettorale, tra le quali si ricordano Giudice di Pace di Napoli, 26 giugno 2004, in *Foro It.*, 2004, c. 2908, la cui massima recita: "Posto che le comunicazioni indesiderate di carattere commerciale effettuate mediante SMS possono costituire interferenza nella sfera privata e arrecare disagi ai destinatari, specie se gestite attraverso sistemi automatici che non implicano l'intervento di un operatore, il fornitore del servizio di telefonia che le abbia realizzate senza prima aver acquisito il consenso espresso del titolare del numero telefonico, è tenuto al risarcimento dei danni ai sensi dell'art. 2043 e 2050 c.c.". Nello stesso senso anche i provvedimenti del Garante della Privacy inerenti agli SMS di propaganda elettorale: Garante Privacy, 7 settembre 2005, in *Cittadini e società dell'informazione*, 2005, doc. web. N. 1165613).

¹²² Giudice di Pace di Padova, 3 febbraio 2004, in *Il diritto della Regione*, 2005, p. 799, con nota di U. Vincenti, *Spamming e indirizzi e-mail conoscibili da chiunque*. In questa decisione il giudice ha

Sotto il profilo contrattuale, la giurisprudenza di merito ha affermato che il rapporto esistente tra il provider e l'utente (titolare di solo indirizzo di posta elettronica e/o di sito web) ha la natura di appalto di servizi. In conseguenza di ciò, rientra tra gli obblighi contrattuali gravanti sul fornitore di servizi anche quello di evitare che l'e-mail account del proprio utente sia esposto allo spamming da parte di altri operatori della Rete¹²³

§5. Conclusioni.

Apparentemente l'aggressivo approccio australiano di contrasto allo *spamming* parrebbe dare i suoi primi frutti, come dimostrato dalla sentenza della *Federal Court of Australia* e dalla cooperazione dei diversi rappresentanti della realtà sociale ed economica del Paese. Ciò nonostante, va sottolineato che il cuore del problema riguarda la notevole quantità di *spam* proveniente da oltremare¹²⁴. Sebbene gli USA si siano dotati di una normativa federale in materia, nota come *Can-Spam Act 2003*¹²⁵, va sottolineato che essa non ha impedito la diffusione dello spam di origine americana in tutto il mondo. Perché questo? Innanzitutto con il *Can Spam Act 2003*, il legislatore federale americano ha deciso che ciascun messaggio elettronico commerciale venga inviato secondo le modalità di *opt out*. Questa scelta è indicativa della *policy* attuata dallo *Can Spam Act 2003*: attraverso la modalità di *opt out* la proliferazione dello *spam* non può essere efficacemente contrastata¹²⁶. Continuando l'analisi dei punti salienti della

rilevato come l'indirizzo e-mail del destinatario fosse conoscibile da chiunque in quanto inserito in un pubblico elenco e quindi non sottoposto ai sensi dell'art. 24, co. 1°, lett. c) al rilascio del consenso preventivo da parte del titolare del dato personale e la mancanza nel sistema di posta elettronica dell'attore di filtri *antispam*. Nello stesso senso, la citata sentenza del GUP di Udine sulla non configurabilità del documento in casi analoghi. Tuttavia questo orientamento si pone in contrasto con le decisioni del Garante della Privacy, il quale ha stabilito che "la disponibilità in Internet degli indirizzi di posta elettronica resi conoscibili attraverso siti *web* va rapportata alle finalità per le quali gli stessi vi sono stati pubblicati. I dati personali resi in tal modo conoscibili in relazione ad eventi e finalità delimitati non sono liberamente utilizzabili per l'invio di e-mail aventi contenuto commerciale o pubblicitario (Garante della Privacy, 25 settembre 2003, in *Cittadini e società dell'informazione*, 2003, doc. web. N. 1082063; Id., 25 settembre 2003, *ibidem*, doc. web. N. 1081990; Id., 25 settembre 2003, *ibidem*, doc. web., 1082023; Id., 22 settembre 2003, *ibidem*, doc. web. N. 1082002; Id., 22 settembre 2003, *ibidem*, 1081823; Id., 22 settembre 2003, *ibidem*, doc. web, N. 1081811

¹²³ Trib. Prato, 15 ottobre 2001, in *Foro toscano*, 2002, p. 100, con nota di E. Olivetti Rason, *Sulla delicata quanto attuale problematica della pubblicità attraverso Internet*; e su *Dir. e prat. soc.*, 2002, fasc. 13, p. 73, con nota di G. Cassano, L. Cimino, *Il fenomeno dello "spamming" e la responsabilità del "provider"*.

¹²⁴ NOIE Report, cit., p. 9.

¹²⁵ *Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003*, consultabile sul sito Internet www.congress.gov

¹²⁶ Critiche rilevanti al *Can Spam Act 2003* riguardano le pene miti per gli *spammers*, e le disposizioni normative redatte in modo poco incisivo (R. Stark, C. E. Kurr, *Using The Securities And Exchange Commission's Statutory Weaponry To Combat Spam*, in *37 U. Tol. L. Rev.* 271 (2006), p. 279). Altra parte della dottrina si esprime in termini di "legge federale debole" (J. M. Blanke, *"Robust Notice" And "Informed Consent:" The Keys To Successful Spyware Legislation*, in *7 Colum.*

normativa federale americana, è previsto che nel messaggio commerciale elettronico venga altresì indicato l'indirizzo del mittente e siano specificati sia le *header*, nonché l'oggetto della comunicazione il quale deve contenere l'indicazione di "advertising", infine l'eventuale contenuto sessuale o pornografico del messaggio deve essere esplicitato. Ulteriormente, il *CAN Spam Act* proibisce l'apertura di indirizzi email multipli con l'utilizzo di informazioni false, nonché la falsificazione degli *header*, l'uso degli *open relays* per inviare comunicazioni commerciali non sollecitate, l'indicazione ingannevole dell'oggetto della comunicazione, l'uso di *harvesting software* per creare mailing list da spammare¹²⁷. Risulterebbe chiaro, quindi, che l'obiettivo dello *CAN Spam Act 2003* è di impedire la diffusione di informazioni commerciali false¹²⁸ e non la diffusione dello *spam* attraverso Internet. Questa è l'antitesi della posizione australiana, la quale considera illecito l'invio dei messaggi commerciali non richiesti.

La soluzione del problema relativo alla proliferazione della posta indesiderata via Internet non sembra possa riferirsi interamente a scelte di *policy* o legislative. Queste presupporrebbero un accordo transnazionale per il raggiungimento di un ampio coordinamento normativo in materia. Tuttavia, detta tematica va osservata in una prospettiva diversa, ovvero quella del cyberspazio, il quale presume il superamento dei limiti derivanti dalla sovranità territoriale¹²⁹. Questa strategia andrebbe coordinata con il perfezionamento delle soluzioni tecniche già in uso, quale per esempio l'adozione di filtri bayesiani, che permettano di intercettare correttamente la posta indesiderata.

Il contrasto allo *spam* è una campagna che merita di essere combattuta nel nome del risparmio di uno dei beni più preziosi e non rinnovabili che ci appartengono: il tempo.

Sci. & Tech. L. Rev. 2; L. Zhang, *The Can-Spam Act: An Insufficient Response To The Growing Spam Problem*, 20 *Berkeley Tech. L.J.* 301 (2005), p. 319.

¹²⁷ R. A. Kurnit, *Advertising And Corporate Communications Liability*, in *SL008 ALI-ABA 431* (2006), p. 431; J. R. Stark, C. E. Kurr, *Using The Securities*, cit., p. 275.

¹²⁸ W. R. Denny, *Electronic Communications With Clients: Minding The Ethics Rules And The Can-Spam Act*, in *62-DEC Bench & B. Minn. 17* (2005), p. 18.

¹²⁹ *Statement By H. E. Mr. Yoshio Utsumi Secretary-General Of The International Telecommunication Union at the World Summit of the Information Society, Tunisi, 16 novembre 2005*, consultabile sul sito Internet www.itu.int.