



Internet: no a e-mail pubblicitarie senza consenso

Non si possono inviare e-mail per pubblicizzare un prodotto o un servizio senza prima aver ottenuto il consenso del destinatario, anche quando si tratta solo del primo invio. Lo ha ribadito il Garante con una [decisione su un ricorso](#) presentato da un persona che aveva ricevuto posta elettronica indesiderata da parte di una società di prodotti informatici che opera in Internet.

L'interessato, infastidito dalla e-mail sgradita, si era rivolto alla società per chiedere, tra l'altro, la cancellazione dei propri dati dall'archivio della società e di adottare misure affinché non si ripetessero in futuro altri invii. Non avendo ricevuto adeguato riscontro, ha presentato ricorso al Garante. E il Garante gli ha dato ragione, imponendo alla società di cancellare dal data base i suoi dati personali. La società si era giustificata spiegando che quel primo invio era volto solo a richiedere il consenso per il successivo inoltro di comunicazioni commerciali. 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.

Ribadendo 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.

"Occorre dire un fermo no - ha commentato Giuseppe Fortunato, relatore del [provvedimento](#) - alla prassi di mandare una mail pubblicitaria senza consenso e poi scusarsi affermando che comunque quella era l'unica comunicazione inviata. Così come bisogna smetterla con la prassi di reperire un indirizzo di posta elettronica su Internet e poi utilizzarlo per mail pubblicitarie non richieste. Il Garante non può tollerare tali comportamenti intrusivi".

APPROFONDIMENTI

Il Garante vara il piano delle ispezioni per il primo semestre 2006

Comunicato stampa - 03 febbraio 2006

Il Garante ha stabilito il programma di accertamenti per il primo semestre del 2006 e ha definito criteri, principi e priorità di intervento per verificare se chi gestisce banche dati raccolga, usi e conservi i dati personali dei cittadini lecitamente e nel rispetto di quanto previsto dalle norme a tutela della privacy.

Avranno priorità le verifiche sulle seguenti modalità e settori:

- siti Internet;
- vendite a distanza;
- case farmaceutiche;
- sistemi di informazioni creditizie.

Le attività di accertamento potranno comportare l'applicazione di sanzioni, il divieto a trattare dati personali senza il rispetto del Codice, e prescrizioni all'uso dei dati personali. Si prosegue pertanto nel potenziamento delle attività ispettive con un articolato ciclo di controlli sul territorio, in vari settori ed aree di intervento, puntando alla verifica del rispetto delle norme da parte di quanti trattano dati personali per la fornitura di beni e servizi mediante varie forme di vendita a distanza e da parte dei siti web. Inoltre verrà verificata la correttezza dei trattamenti effettuati da società farmaceutiche e la gestione dei dati personali da parte di banche o finanziarie relativi alle segnalazioni nei sistemi di informazioni creditizie.

Altre ispezioni riguarderanno soggetti privati e pubbliche amministrazioni per accertare in particolare il rispetto degli obblighi di notificazione, cioè la comunicazione al Garante da parte di determinati soggetti dell'avvio di una banca dati, e di informazione ai cittadini sull'uso che verrà fatto dei loro dati. Infine continueranno le eventuali attività ispettive che si rendessero necessarie in sede istruttoria su reclami, segnalazioni o ricorsi, nonché le attività svolte in collaborazione e su richiesta dell'autorità giudiziaria penale. Le ispezioni verranno effettuate direttamente presso le sedi dove si svolgono i trattamenti di dati personali anche in collaborazione con il Nucleo speciale funzione pubblica e privacy della Guardia di Finanza.

Proprio allo scopo di dare ancora maggiore sviluppo alla collaborazione con la Guardia di Finanza e di intensificare l'attività di vigilanza e controllo sul rispetto delle norme, anche alla luce delle modifiche intervenute con il Codice sulla protezione dei dati personali, nei mesi scorsi è stato sottoscritto un nuovo protocollo di intesa con la Guardia di Finanza che prevede l'impiego, oltre che del Nucleo speciale funzione pubblica e privacy, anche dei reparti territoriali del Corpo. Nel 2004 il Garante ha concluso 100 ispezioni, mentre nel 2005 ne sono state effettuate 230, con l'applicazione di sanzioni per 4,2 milioni di Euro.



Codice in materia di dati personali

“APPROFONDIMENTI”

 **Troppi dati agli sportelli bancari e postali - N. 267 del 25 novembre 2005**

Occorre maggiore sobrietà nella richiesta dei documenti di identificazione

Banche ed uffici postali devono limitare ai soli casi indispensabili la richiesta di documenti di riconoscimento dei loro clienti. Inoltre, non sempre è necessario trattenere la fotocopia del documento per effettuare operazioni bancarie o postali: ad esempio, per il pagamento di un assegno o di un vaglia postale è spesso sufficiente l'esibizione di un documento di identità. Occorre anche evitare di acquisire più volte copia dei documenti già disponibili.

Lo ha precisato il Garante, a seguito di segnalazioni di numerosi cittadini, con un provvedimento con il quale ha prescritto a banche e uffici postali di adottare modalità proporzionate nella richiesta di identificazione dei clienti e di limitarsi a conservare copia del documento solo nei casi stabiliti dalla legge.

L'interessato, ha spiegato il Garante, va identificato rispettando il principio di pertinenza e proporzionalità evitando richieste eccessive di dati e basandosi, caso per caso, su diversi elementi di valutazione come la conoscenza personale, atti o documenti acquisiti in precedenza, l'esibizione del documento o l'eventuale annotazione degli estremi sul documento.

La produzione, anche in via telematica, di una copia del documento di riconoscimento e la sua conservazione sono giustificate, ha sottolineato il Garante, solo se previste espressamente da una norma o solo se la banca o l'ufficio postale devono dimostrare di aver identificato l'interessato relativamente ad alcune particolari operazioni (ad es., un cliente sconosciuto che presenta un assegno) con modalità più accurate.

Va ricordato che l'identificazione è spesso prevista da norme oppure è necessaria per eseguire gli obblighi del contratto e non richiede quindi il consenso dell'interessato.

Il Garante ha richiamato infine l'attenzione sulla necessità di adottare opportune cautele affinché si evitino inutili letture dei dati che permettano l'ascolto da parte di soggetti estranei, assicurando sempre l'opportuno riserbo nelle operazioni di sportello.

"La necessità del rispetto del cittadino che consegna propri documenti a istituti bancari e uffici postali – ha affermato il componente dell'Autorità, Giuseppe Fortunato, relatore del provvedimento – ha ispirato uno specifico provvedimento del Garante circa le modalità per l'identificazione dei clienti. Più copie degli stessi documenti, lettura dei documenti dinanzi ad altri clienti, impiegati che conservano copie dei documenti senza che ve ne sia necessità, utilizzo ad altri fini dei documenti raccolti testimoniano spesso la poca consapevolezza del rispetto della dignità delle persone e, come ha voluto esplicitamente prescrivere il Garante, non sono modalità permesse".



Codice in materia di dati personali

“APPROFONDIMENTI”

 **Propaganda elettorale: il "decalogo" del Garante – Comunicato Stampa 10 febbraio 2006**

Liberi gli indirizzi delle liste elettorali, serve il consenso per sms ed e-mail

Regole chiare per partiti e candidati e garanzie a tutela dei diritti dei cittadini. In vista dell'avvio della campagna elettorale, il Garante Privacy, composto da Francesco Pizzetti, Giuseppe Chiaravalloti, Mauro Paissan e Giuseppe Fortunato, richiama l'attenzione sulle modalità in base alle quali chi effettua propaganda elettorale potrà utilizzare correttamente i dati personali dei cittadini (ad es. indirizzo, telefono, e-mail etc.). Le prescrizioni sono contenute nel recente provvedimento generale adottato in materia.

Dati utilizzabili senza consenso

Per contattare gli elettori ed inviare materiale di propaganda partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono usare **senza il consenso dei cittadini** i dati contenuti nelle **liste elettorali** detenute dai Comuni. Possono essere usati anche altri elenchi e registri in materia di elettorato passivo ed attivo (es. **elenco degli elettori italiani residenti all'estero**) ed altre fonti documentali detenute da soggetti pubblici accessibili a chiunque (es. **albi professionali**). Partiti e candidati possono usare lecitamente i dati personali di **iscritti ed aderenti**.

Per i titolari di cariche elettive vi è la possibilità di utilizzare informazioni raccolte nel quadro delle relazioni interpersonali da loro avute con cittadini ed elettori.

Dati utilizzabili con il previo consenso

A meno che i dati personali siano stati forniti direttamente dall'interessato, è **necessario il consenso** per particolari modalità di comunicazione elettronica come **sms, e-mail, mms**, per **telefonate preregistrate** e **fax**. Stesso discorso nel caso si utilizzino dati raccolti automaticamente su Internet o ricavati da forum o newsgroup, liste abbonati ad un provider, dati presenti sul web per altre finalità.

Sono utilizzabili anche i dati degli abbonati presenti nei **nuovi elenchi telefonici** accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere posta o telefonate. Sono ugualmente utilizzabili, se si è ottenuto preventivamente il consenso degli interessati, i dati relativi a **simpatizzanti** o altre persone già contattate per singole iniziative o che vi hanno partecipato (es. referendum, proposte di legge, raccolte di firme).

Dati non utilizzabili

Non sono in alcun modo utilizzabili, neanche da titolari di cariche elettive, gli **archivi dello stato civile**, l'anagrafe dei residenti, **indirizzi raccolti per svolgere attività e compiti istituzionali o per prestazioni di servizi, anche di cura**.

Informazione ai cittadini

I cittadini devono essere informati sull'uso che si fa dei loro dati. Se i dati non sono raccolti direttamente presso l'interessato, l'informativa va data al momento del primo contatto o all'atto della registrazione. Per i dati raccolti da registri ed elenchi pubblici o in caso di invio di materiale propagandistico di dimensioni ridotte



Codice in materia di dati personali

“APPROFONDIMENTI”

(c.d. "santini"), il Garante ha consentito a partiti e candidati una temporanea sospensione dell'informativa fino al 30 giugno 2006.

 **Recupero crediti: il Garante, no a comportamenti che ledono la dignità – Comunicato
Stampa 20 gennaio 2006**

Il Garante per la privacy (composto da Francesco Pizzetti, Giuseppe Chiaravallotti, Mauro Paissan, Giuseppe Fortunato) ha adottato un provvedimento a carattere generale con il quale ha prescritto alle società di recupero crediti e a quanti - finanziarie, banche, concessionari di pubblici servizi, compagnie telefoniche - svolgono tale attività direttamente, le misure alle quali attenersi per non incorrere in illeciti e per rispettare i principi posti a tutela dei diritti dei cittadini.

Le prescrizioni del Garante

Non sono ammesse prassi invasive o lesive della dignità personale. Per sollecitare ed ottenere il pagamento di somme dovute non è lecito comunicare ingiustificatamente informazioni relative ai mancati pagamenti ad altri soggetti che non siano l'interessato (es. familiari, colleghi di lavoro o vicini di casa) ed esercitare indebite pressioni su quest'ultimo. Non si deve far ricorso a telefonate preregistrate perché con questa modalità persone diverse dal debitore possono venire a conoscenza di una sua eventuale condizione di inadempienza. Illecita è pure l'affissione da parte degli incaricati del recupero crediti di avvisi di mora sulla porta di casa, modalità questa che rende possibile la diffusione dei dati personali dell'interessato ad una serie indeterminata di soggetti.

Non si deve inoltre rendere visibile a persone estranee il contenuto di una comunicazione, come può accadere con l'utilizzo di cartoline postali o con l'invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili. È necessario, invece, che le sollecitazioni di pagamento vengano portate a conoscenza del solo debitore, usando plichi chiusi e senza scritte specifiche. Gli incaricati delle società non possono usare altri dati se non quelli assolutamente necessari all'esecuzione del mandato (dati anagrafici, codice fiscale, ammontare del credito, recapiti telefonici). Una volta assolto l'incarico e acquisite le somme, i dati devono essere cancellati. L'intervento del Garante è giunto al termine di accertamenti avviati dall'Autorità dopo che numerosi cittadini e associazioni a tutela dei consumatori avevano segnalato un uso illecito dei loro dati personali nell'attività di recupero crediti. In particolare, veniva lamentato come attraverso gli incaricati venissero messe in atto modalità di ricerca, presa di contatto, sollecitazione al pagamento delle somme dovute, particolarmente invasive: visite a domicilio o sul posto di lavoro; reiterate sollecitazioni al telefono fisso o sul cellulare; telefonate preregistrate; invio di posta con l'indicazione all'esterno della scritta "recupero crediti" o "preavviso esecuzione notifica", fino all'affissione di avvisi di mora sulla porta di casa. Spesso, inoltre, dati personali di intere famiglie risultavano inseriti nei data base del soggetto creditore o delle società di recupero crediti.



 **Misure di sicurezza e Dps: Prorogati i termini – News 04 gennaio 2006**

Publicato il decreto legge di proroga di alcuni termini
(D.l. 30 dicembre 2005, n. 273, in G.U. 30 dicembre 2005, n. 303)

È stato pubblicato sulla *Gazzetta Ufficiale* del 30 dicembre 2005 il decreto-legge che proroga alcuni termini per le misure minime di sicurezza (presso soggetti pubblici e privati) e per il trattamento dei dati sensibili e giudiziari (presso soggetti pubblici).

La proroga disposta dal decreto legge riguarda *solo* due aspetti:

a) le *nuove* misure minime di sicurezza

È stato differito al *31 marzo 2006* il termine per adottare le nuove misure minime di sicurezza non previste dalla disciplina precedente al Codice. Simmetricamente, è differito al 30 giugno 2006 un termine di legge connesso. Di questo differimenti possono beneficiare soggetti pubblici e privati (v. art. 180 del Codice);

b) il termine per adottare i regolamenti nelle p.a. sui dati sensibili e giudiziari
I soggetti pubblici hanno tempo sino al 28 febbraio 2006 per adottare e rendere pubblici i regolamenti che individuano i tipi di dati sensibili e giudiziari trattati e di operazioni eseguite. (v. art. 181 del Codice).



Codice in materia di dati personali

“APPROFONDIMENTI”