GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Newsletter - 21 marzo 2005

Newsletter NOTIZIARIO SETTIMANALE
ANNO VII
WWW.GARANTEPRIVACY.IT

N. 249 del 21 - 27 marzo 2005

Internet: motori di ricerca e diritto all'oblio

Soluzione tecnica individuata dal Garante per garantire la trasparenza, ma evitare le "gogne" elettroniche

É legittimo che una sanzione, una condanna o un altro precedente "pregiudizievole" lontani nel tempo siano per sempre disponibili a tutti e a chiunque in Internet tramite i comuni motori di ricerca? Trascorso un congruo periodo di tempo, si ha il diritto di "uscire" da questo spazio di Internet, nel senso che i documenti ufficiali che non hanno più attinenza con l'attualità siano resi trasparenti, anche sul web, ma in modo più selettivo, dando a quei precedenti la giusta dimensione che contenga danni e pregiudizi? Al diritto all'oblio, riconosciuto dal Codice in materia di protezione dei dati personali, si è appellato un operatore pubblicitario, che ha presentato ricorso al Garante chiedendo di disporre nei confronti di un ente pubblico gli opportuni accorgimenti per interrompere quella che riteneva una perpetua "gogna" elettronica.

Il Garante (con una decisione adottata dal precedente collegio) gli ha dato in parte ragione e ha previsto che l'ente continui a divulgare sul proprio sito istituzionale le decisioni sanzionatorie riguardanti l'interessato e la sua società, ma - trascorso un congruo periodo di tempo - collochi quelle di vari anni or sono in una pagina del sito accessibile solo dall'indirizzo web. Tale pagina, ricercabile nel motore di ricerca interno al sito, dovrà essere esclusa, invece, dalla diretta reperibilità nel caso si consulti un comune motore di ricerca, anziché il sito stesso.

Il ricorrente lamentava il fatto che chiunque effettuasse in rete una normale ricerca nominativa a nome suo e della società, tramite uno dei comuni motori di ricerca in Internet, ricevesse sempre e in primo luogo non le notizie riguardanti la sua attuale o più recente attività professionale, ma due provvedimenti con i quali gli erano state a suo tempo applicate due sanzioni amministrative, una delle quali risalenti al 1996 e l'altra al 2002. Ciò, sosteneva l'interessato, pregiudicava l'immagine che la clientela poteva farsi dell'attività da lui svolta.

Il ricorrente e la sua società non contestavano né le sanzioni, né il fatto che l'ente dovesse pubblicarle ufficialmente anche sul sito istituzionale. Si opponevano, invece, a che i provvedimenti stessi fossero reperibili indiscriminatamente in Internet sempre e da chiunque, anche da persone che non avessero consultato il sito dell'ente e fossero semplicemente intente a contattare la società. Si chiedeva, quindi, l'adozione di opportune cautele, quali potevano essere, in alternativa all'oscuramento del nominativo, un accesso meno "diretto" alle pagine web in questione.

L'ente pubblico ha fatto presente i propri obblighi nel pubblicizzare le decisioni adottate nel proprio Bollettino Ufficiale e sul sito, rappresentando l'interesse pubblico alla piena conoscibilità, anche nel tempo, delle sue decisioni: omettendo invece le generalità del ricorrente e della sua società, sarebbe stato pressoché inutile per i cittadini interessati consultare le decisioni che mirano proprio ad informare specificamente sulle violazioni amministrative. L'ente ha dato la sua immediata disponibilità a ricercare gli opportuni accorgimenti e, su questa base, è stato avviato un delicato accertamento tecnico. Diverse ipotesi non risultavano tecnicamente praticabili o soddisfacenti. Né si poteva ignorare la circostanza che per le decisioni dei soggetti pubblici non è obbligatoria la cautela di omettere i nominativi nelle decisioni pubblicate, ipotesi prevista dal Codice in materia di protezione dei dati personali solo per le sentenze dell'autorità giudiziaria accessibili in Internet.

Il Garante ha disposto, dunque, che l'ente pubblico continui a pubblicare sul proprio sito le proprie decisioni, anche a distanza di tempo, predisponendo però nell'ambito del proprio sito web, entro un trimestre, una sezione per i vecchi provvedimenti (dove collocare ad esempio la predetta decisione del 1996) consultabile da tutti tramite il sito, ma attraverso l'indirizzo dell'ente, anziché mediante una domanda a tappeto tramite i motori esterni di ricerca.

Entro lo stesso termine, l'ente individuerà altresì il periodo temporale, proporzionato al raggiungimento delle proprie finalità durante il quale i propri provvedimenti saranno liberamente reperibili in Internet anche tramite motori di ricerca (come ancora avviene per la predetta decisione del 2002).

Si tratta di una decisione "pilota" che avvia una nuova complessa riflessione tra trasparenza e oblio alla luce delle diverse opportunità offerte da Internet.

"Etichette intelligenti": le garanzie per il loro uso

Quando si trattano dati personali, i cittadini devono essere informati, esprimere un libero consenso e poter disattivare i chip

Sono precise le garanzie e le prescrizioni impartite dal Garante per chi intende produrre ed utilizzare le cosiddette "etichette intelligenti", cioè quei minuscoli chip a radiofrequenza (detti anche sistemi *Rfid, Radio Frequency Identification*) attivati da lettori ottici, che iniziano a trovare applicazione anzitutto nell'ambito delle aziende, degli esercizi commerciali, della grande distribuzione allo scopo di ottenere una serie di vantaggi, anche per il consumatore (migliore gestione dei prodotti aziendali, maggiore rapidità delle operazioni commerciali, agevole rintracciabilità dell'origine di particolari prodotti, controllo degli accessi a luoghi riservati).

Alcuni impieghi di questa tecnologia - che non si limitino a tracciare il prodotto per garantire l'efficienza del processo di produzione industriale - possono costituire una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone: con l'uso di *Rfid* si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori **a fini di profilazione o essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usa, indossa, trasporta**.

I sistemi *Rfid* possono essere usati anche da soggetti pubblici o privati anche ad altri scopi, quali l'identificazione personale o la tutela della salute. Alcuni particolari usi, come l'impianto di **microchip sottopelle**, sollevano già oggi problematiche di grande delicatezza che hanno già indotto altre autorità garanti in Europa a considerarlo inaccettabile sul piano della protezione dei dati personali.

Ulteriori pericoli possono derivare dall'adozione di *standard* comuni tali da favorire la possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (es. mediante la loro riscrittura). I rischi possono accrescersi nel caso si integrino le tecniche *Rfid* con infrastrutture di rete, come telefonia ed Internet e sulla base dello stesso sviluppo tecnologico che, potenziando i sistemi, può consentire **una "lettura" delle etichette a distanze sempre maggiori**.

É per questi motivi che il Garante ha adottato un provvedimento generale, del quale è stato relatore Stefano Rodotà e che si collega a quello varato di recente dai garanti europei, per stabilire alcune prime misure per rendere conformi l'impiego dei sistemi *Rfid* alle norme sulla privacy nei casi in cui si trattino dati personali relativi a persone identificate o identificabili e tutelare la loro dignità e la libertà.

Informativa

Le persone devono essere adeguatamente informate dell'utilizzo di sistemi *Rfid,* così come dell'esistenza dei lettori ottici che attivano l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche *Rfid* sono utilizzate non esime da apporre informativa sugli stessi oggetti e prodotti che recano le etichette intelligenti.

Consenso

Un soggetto privato che utilizza *Rfid* trattando dati personali può farlo **solo con il consenso espresso e specifico degli interessati**, a meno che ricorra in casi particolari uno degli altri presupposti di legge. Il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato.

Se le etichette intelligenti sono associate all'utilizzo di carte di fedeltà, e si trattano dati a fini di profilazione dei consumatori, occorre informare e acquisire il consenso degli interessati.

Il consenso non è necessario quando le etichette intelligenti sono adoperate solo per modalità di pagamento e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili.

Disattivazione

Alle persone deve essere garantito comunque il **diritto di asportare, disattivare o interrompere gratuitamente ed in maniera agevole il funzionamento** delle *Rfid* al momento dell'acquisto del prodotto sui cui è apposta l'etichetta. Le etichette devono essere posizionate in modo tale da risultare facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto (es. collocate solo sulla confezione).

Non è, di regola, lecita l'installazione di Rfid destinate a rimanere attive oltre la barriera-cassa dell'esercizio commerciale.

Accesso a determinati luoghi o a posti di lavoro

Nei casi di impiego di *Rfid* per la verifica di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà delle persone. In particolare: per i luoghi di lavoro va rispettato quanto previsto dallo **Statuto dei lavoratori che vieta l'utilizzo di impianti per il controllo a distanza dei lavoratori**; per l'accesso occasionale di terzi a determinati luoghi occorre predisporre un meccanismo che, nel caso di indisponibilità ad usare *Rfid* da parte dell'interessato, gli permetta comunque di entrare nel luogo in questione.

Microchip sottopelle

Tali impianti devono ritenersi **in via di principio esclusi** in quanto in contrasto con i diritti, le libertà fondamentali e la dignità della persona. Essi possono essere ammessi **solo in casi eccezionali per comprovate e giustificate esigenze di tutela della salute** delle persone. L'interessato, comunque, deve poter **ottenere la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano**. Si devono prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato.

Va ricordato che anche nei casi di un limitato impiego di microprocessori sottocutanei (es. Stati Uniti), sono stati messi in evidenza i potenziali rischi sia per la salute che soggetti che si sottopongono all'impianto, sia per la sicurezza dei dati personali trattati.

Il Garante ha stabilito, comunque, che i soggetti che intendono utilizzare tali microchip devono **sottoporre alla**

verifica preliminare dell'Autorità tali sistemi.

Proporzionalità, finalità di raccolta e conservazione dei dati
L'uso di etichette intelligenti deve risultare proporzionato agli scopi che si intende perseguire. I dati possono essere utilizzati solo per le finalità per le quali sono stati raccolti e devono essere conservati per il tempo strettamente necessario.

Misure di sicurezza
Chi utilizza etichette intelligenti e tratta dati personali ha l'obbligo di adottare misure di sicurezza per ridurre i rischi di distruzione, perdita, acceso non autorizzato o manomissione dei dati conservati.

Notificazione
L'avvio di trattamenti di dati che indicano la posizione geografica di persone o oggetti mediante reti di comunicazione elettronica o che siano effettuati allo scopo di costruire profili o personalità di un individuo devono essere comunicati preventivamente al Garante.

NEWSLETTER
del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).
Direttore responsabile: Baldo Meo.
Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.
Tel: 06.69677.1 - Fax: 06.69677.785
Newsletter è consultabile sul sito Internet www.garanteprivacy.it

stampa **chiudi**