40 TV interattiva e trattamento dei dati 3 febbraio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Esaminati i reclami e le segnalazioni pervenuti in ordine al trattamento di dati personali in relazione alla prestazione di servizi televisivi interattivi o ad accesso condizionato;

Ritenuta la necessità di prescrivere alcune misure necessarie ed opportune al fine di rendere il trattamento di tali dati conforme alle disposizioni vigenti (art. 154, comma 1, lett. *c*), del Codice in materia di tutela dei dati personali);

Vista la documentazione acquisita a seguito degli accertamenti avviati e della consultazione pubblica effettuata;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Mauro Paissan;

PREMESSO

1. Nuovi servizi televisivi

La crescente integrazione tra le più recenti tecnologie utilizzate nella televisione, nelle comunicazioni elettroniche e nell'informatica rende disponibili prodotti e servizi innovativi basati anche sullo sviluppo di tecnologie digitali. Utenti e abbonati possono usufruire di svariati prodotti anche interattivi, accessibili via etere (terrestre o satellitare) o via cavo, utilizzando soluzioni a pagamento (abbonamento, *pay per view* e *video on demand,* ecc.) o altre forme di accesso condizionato.

Per usufruire di servizi e prodotti ci si deve dotare di un *decoder* o *set-top-box* che rende visibili segnali anche criptati ed è collegabile a una linea telefonica comunicazione dati (*cd.* "canale di ritorno"). Si può in tal modo comunicare con il fornitore del servizio attraverso un telecomando o un'apposita tastiera, inviando richieste o informazioni secondo diversi livelli di interazione. In tal modo è così possibile visionare film ed eventi sportivi, partecipare a sondaggi, giochi o *test*, formare palinsesti personalizzati, accedere a servizi di *telebanking*, televendita, ecc. Abbonati e utenti assumono così un ruolo attivo nei rapporti con i fornitori, interagiscono con essi in un'ottica di crescente personalizzazione e sono talvolta identificati nominativamente.

Le prescrizioni del presente provvedimento riguardano in termini generali tutti i predetti ambiti, diversi dai tradizionali servizi di radiodiffusione che vengono offerti ad un pubblico indifferenziato senza identificare gli utenti. Si prescinde, quindi, dalla tecnologia impiegata per prestare il servizio, dalla tecnica di trasmissione (analogica o digitale), dalla modalità di pagamento prescelta (*es.*, carte prepagate) o dai dispositivi utilizzati (digitazione di una tastiera o telecomando, ecc.). In presenza di un canale di ritorno sempre attivo, i servizi televisivi interattivi offerti via cavo permettono maggiori opportunità di costante monitoraggio e profilazione (non richiedendo l'attivazione reiterata del canale di ritorno) e presuppongono, pertanto, maggiori cautele nell'attuazione delle prescrizioni di seguito indicate.

Richiedono, poi, ulteriore considerazione in altra sede le specifiche problematiche poste

(*) [doc. web n. 1109503 vers. EN n. 1116787]

dal possibile coinvolgimento delle reti di telefonia mobile (anche per quanto riguarda l'identificazione della linea chiamante) o dall'offerta di altri tipi di servizi (come quelli sanitari, che comportano il trattamento di dati sensibili, o come quelli che permettono di accedere ad alcuni servizi di pubblica utilità attualmente in fase di sperimentazione, specie in sede locale: richiesta di certificati o documenti amministrativi o di svolgimento di pratiche, accesso a canali civici, ricerche in banche dati, ecc.). In questi casi, si pongono infatti problemi particolari specie per quanto riguarda i flussi di dati, l'informativa e l'eventuale richiesta di consenso.

Il Garante esamina qui i profili di competenza rilevanti per il trattamento dei dati personali, considerando che la necessità di assicurare agli utenti un livello elevato di tutela dei loro diritti e libertà fondamentali (nonché della dignità), affermata dal Codice in materia (d.lg. n. 196/2003), è stata ribadita da recenti norme sull'assetto del sistema radiotelevisivo (art. 4, comma 3, l. 3 maggio 2004, n. 112).

La possibilità che l'abbonato o l'utente trasmettano inconsapevolmente, mediante il canale di ritorno (ovvero via cavo), svariate informazioni che li riguardano -e che possono essere inviate da differenti utenti anche in ambito familiare- rende necessario individuare specifiche garanzie volte a prevenire illecite operazioni di profilazione e forme invasive di controllo su gusti e abitudini di persone, le quali vanno poste in grado di effettuare le proprie scelte liberamente e in modo informato.

A garanzia degli interessati, il Garante prescrive quindi ai titolari del trattamento di adottare alcune misure necessarie od opportune al fine di conformare i trattamenti alle vigenti disposizioni in materia di protezione dei dati personali (art. 154, comma 1, lett. *c*), del Codice), che sono applicabili anche nella parte riguardante le comunicazioni elettroniche (Titolo X, artt. 121 ss.), quando vengono in considerazione abbonati o utenti riceventi identificati o identificabili (*cfr.* art. 4, comma 2, lett. *a*)).

2. Necessità e proporzionalità

Il trattamento dei dati deve rispettare i principi di necessità, liceità, correttezza, qualità dei dati e di proporzionalità (artt. 3 e 11 del Codice).

In particolare:

- applicando il principio di necessità (art. 3 del Codice), i sistemi informativi e i programmi informatici devono essere configurati, già dall'origine, in modo da ridurre al minimo l'utilizzo delle informazioni relative ad abbonati ed utenti identificabili. Il trattamento di tali informazioni non è lecito se le finalità possono essere perseguite utilizzando solo dati realmente anonimi o indirettamente identificativi;
- nel rispetto del principio di proporzionalità nel trattamento (art. 11, comma 1, lett. *d*), del Codice), tutti i dati personali e le varie modalità del loro trattamento nelle singole fasi ed occasioni di utilizzazione devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

All'atto dell'eventuale acquisto di un *decoder* o di un *set top box* va distinto il caso in cui si debba contestualmente instaurare necessariamente un rapporto contrattuale con un abbonato identificato, dalle ipotesi nelle quali tale identificazione (e la possibile associazione tra nominativo e numero seriale dell'apparecchio *decoder*) non è lecita, essendo ad esempio il *decoder* utilizzato solo con schede prepagate non identificative.

Anche nel caso in cui eventuali e specifici obblighi di legge prescrivano puntualmente di identificare l'acquirente, occorre valutare le finalità di tale identificazione, che potrebbe essere eventualmente prescritta solo a fini fiscali di documentazione giustificativa per eventuali contributi statali. Dal punto di vista della protezione dei dati personali devono ritenersi parimenti illecite eventuali banche dati di titolari possessori di antenne televisive o satellitari, a prescindere dall'eventuale, e più problematica, associazione di tali dati ad altre informazioni personali.

Rispetto alle garanzie previste dal Codice è più indicata l'utilizzazione di carte prepagate impersonali, in luogo di abbonamenti nominativi.

Se ricorrono necessità di fatturazione non è poi lecito trattare eventuali dati personali relativi a tempi di connessione, visioni di programmi ed eventi, fasce orarie di utilizzazione del mezzo televisivo, interruzioni di ascolto, cambi di canale ed analisi del comportamento in presenza di spazi pubblicitari, se non nella misura, modalità e tempi effettivamente necessari.

L'eventuale richiesta –rivolta dal fornitore ai singoli utenti– di identificarsi nominativamente al momento in cui essi inviano informazioni attraverso il canale di ritorno è lecita solo se sottoposta all'esame preliminare di questa Autorità (art. 17 del Codice).

In occasione di altri eventi di *cd.* televoto deve essere evitata, fin dal momento della ricezione delle informazioni trasmesse dall'utente, la raccolta e/o la registrazione di dati associabili a persone identificabili, anche quando le domande riguardino solo gradimenti, gusti o preferenze e non siano richieste anche opinioni di natura sensibile su persone, fenomeni sociali o profili politico-religiosi o sindacali. Ricerche di mercato, altre ricerche campionarie e sondaggi devono essere effettuati in forma anonima, evitando l'afflusso di risposte relative a soggetti identificabili, oppure (se ciò è tecnicamente inevitabile) rendendo tali risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali.

Infine, non ogni richiesta degli utenti o acquisto di determinati prodotti o partecipazione a sondaggi determinano, di per sé stessi, il trattamento di dati sensibili. Nel caso in cui, per le specifiche informazioni trasmesse dagli utenti o per le modalità della loro utilizzazione si intenda raccogliere dati sensibili (art. 4, comma 1, lett. *d*), del Codice), deve tenersi presente che il loro trattamento non è di regola ammesso né per l'ordinaria prestazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, fatta salva l'ipotesi eccezionale nella quale il medesimo trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che acconsentito dall'interessato in forma scritta o telematica equiparabile allo scritto. Ciò, vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie *(cfr. Autorizzazione generale* del Garante n. 5/2004, in *G.U.* 14 agosto 2004, n. 190).

3. Informativa

L'informativa ora fornita all'atto della richiesta della *smart card* non è idonea in rapporto alla delicatezza e complessità dei flussi di informazioni, i quali possono peraltro riguardare più utenti facenti capo ad un medesimo abbonato e permettere a posteriori una ricostruzione dei loro comportamenti anche in ambito domestico, non solo, quindi, dal fornitore in occasione della fatturazione. Finalità e modalità del trattamento dei dati potrebbero inoltre differire da caso a caso, oltre che nel tempo.

Prima della costituzione del rapporto contrattuale, l'abbonato deve ricevere un'informativa chiara e completa, al fine di aderire in modo pienamente consapevole alle iniziative proposte.

Nel rispetto del principio di correttezza (art. 11, comma 1, lett. *a*), del Codice), al pari di quanto già prescritto da questa Autorità a proposito delle iniziative di fidelizzazione *(Provv.* 24 febbraio 2005, in *www.garanteprivacy.it* [doc. *web* n. 1103045]), deve ritenersi non consentito al fornitore di adottare comportamenti suscettibili di incidere sulle scelte libere e consapevoli degli abbonati rispetto ad eventuali iniziative di profilazione che portino, anche attraverso codici numerici, a monitorare le scelte degli interessati e la loro sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo).

L'informativa fornita sia al momento della costituzione del rapporto contrattuale, sia successivamente, riveste particolare importanza, considerati i rischi di sottovalutazione o di errore da parte dell'interessato.

Non è corretto indurre l'abbonato o l'utente a fornire informazioni personali senza aver avuto le spiegazioni e il tempo necessari per essere adeguatamente informati e maturare -allorché ciò è necessario- un consenso consapevole.

Si possono utilizzare formule sintetiche e colloquiali, purché chiare e inequivoche. L'informativa deve contenere tutti gli elementi richiesti dal Codice (art. 13, comma 1), evitando rinvii generici a regolamenti di servizio non acclusi per le parti di riferimento; deve specificare, altresì, la natura dei dati di traffico trattati e la durata del loro trattamento (art. 123, comma 4, del Codice).

L'informativa inserita all'interno di moduli deve essere adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito riquadro, e risultare altresì agevolmente individuabile rispetto ad altre clausole del regolamento di servizio eventualmente riportato in calce o a margine.

La persona fisica che accede ai servizi interattivi, o che viene abilitata caso per caso all'accesso condizionato (sia essa l'abbonato o meno), deve essere informata nuovamente in modo rapido e con brevi frasi efficaci circa l'eventuale utilizzo di dati personali, con una schermata di primo avviso (del tipo: "*Ecco come sono utilizzati i tuoi dati personali*") che permetta, premendo un tasto, di accedere ad un'idonea informativa leggibile anche a distanza.

4. Consenso

Il trattamento di eventuali dati personali preordinato strettamente alla prestazione di servizi richiesti è "*necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato*". In questi casi, non è corretto che il fornitore del servizio solleciti il consenso al trattamento, tantomeno in termini generali (art. 24, comma 1, lett. *b*), del Codice).

Se si pone in essere un'eventuale monitoraggio o profilazione, o si intende cedere dati personali a terzi specificamente individuati, queste circostanze e le relative finalità devono essere indicate puntualmente e con evidenza sia all'atto della costituzione del rapporto, sia prima di evadere le singole richieste di servizio o sollecitare le risposte degli utenti. Deve risultare chiara la circostanza che per questi scopi (come pure per la partecipazione a sondaggi che devono avere scopi fini chiaramente determinati e legittimi), il conferimento dei dati e il consenso sono liberi e facoltativi rispetto all'ordinaria prestazione dei servizi, e non possono ottenersi sulla base di pressioni o condizionamenti.

Nell'interfaccia grafica contenente il menzionato supplemento di informativa all'utente deve apparire l'indicazione su come acconsentire allo specifico trattamento, premendo ad esempio un tasto.

L'indicazione La comunicazione in modalità interattiva di dati sensibili da parte dell'utente al fornitore deve essere possibile solo mediante credenziali di autenticazione associate ad una parola chiave riservata.

5. Pagamenti e fatturazione

L'accesso ai servizi televisivi interattivi e ad accesso condizionato può essere gratuito o comportare specifici pagamenti aggiuntivi, attraverso carte pre-pagate o addebiti periodici (abbonamento o *pay per view*).

Mentre utilizzando carte prepagate il credito viene scalato in automatico, in caso di abbonamento la fattura può indicare gli eventuali "eventi" *pay per view* da pagare.

Essendo possibile che soggetti diversi accedano al medesimo apparecchio televisivo e, dunque, ai servizi televisivi, il fornitore deve porre in essere adeguate misure ed operare un corretto bilanciamento fra la tutela della riservatezza degli effettivi fruitori dei servizi e l'esigenza dell'abbonato di verificare la correttezza degli addebiti.

In applicazione dei menzionati principi di proporzionalità e necessità, i dati che compaiono nelle fatture non devono risultare eccedenti rispetto alla finalità perseguita. Deve essere offerta all'abbonato la possibilità di non ricevere una fatturazione dettagliata. I servizi *pay-per-view* devono essere menzionati per importo totale, data e costo di fruizione, indicando solo su successiva richiesta i "titoli" specifici dei singoli "eventi" acquistati.

40

6. Conservazione dei dati

Nella prestazione di servizi televisivi interattivi o ad accesso condizionato sono trattate tipologie diverse di dati, per differenti finalità.

Accanto a dati "amministrativi" di carattere generale, sono a volte trattati dati inerenti alla fatturazione di singoli consumi televisivi, i quali rilevano in determinati casi come "*dati di traffico*" *(cfr.* art. 4, comma 2, lett. *h*) del Codice), anche quando siano trattati dal fornitore del servizio, oltre che dal gestore telefonico (ad esempio, il numero telefonico o il numero della *smart card*; ora di inizio e durata della comunicazione elettronica relativa al servizio richiesto). Talvolta, come si è visto, possono venire in rilievo anche dati sensibili.

In applicazione del menzionato principio di proporzionalità, va prescritta ai titolari del trattamento l'identificazione di termini massimi di conservazione dei dati, anche nel corso del rapporto.

Tale identificazione va effettuata dopo aver esaminato la possibilità di raccogliere lecitamente e conservare dati nei termini consentiti per ciascuna delle finalità del trattamento che si intende effettuare, tenendo conto di eventuali scelte degli interessati sopravvenute.

Il principio da osservare è quello secondo cui i dati personali dei quali non è necessaria la conservazione in relazione agli scopi per i quali essi sono stati raccolti o successivamente trattati devono essere cancellati o trasformati in forma anonima (art. 11, comma 1, lett. *e*), del Codice).

Se non ricorrono esigenze di specifica fatturazione dei singoli prodotti, e non vi è un distinto e specifico consenso alla profilazione, i dati personali desumibili dal voto televisivo, da sondaggi, acquisti, ecc. non possono essere registrati ed utilizzati per l'una o l'altra di queste finalità.

Decorso il termine per le singole fatturazioni e le relative contestazioni, i dati personali relativi ai singoli servizi o programmi acquistati devono essere cancellati. La cancellazione deve riguardare anche la memorizzazione del consenso -acquisito nei soli casi in cui esso è, come si è detto, necessario- manifestato in forma scritta o telematica equiparabile allo scritto.

Anche laddove sia stato acquisito uno specifico consenso, di dati di dettaglio su acquisti e servizi possono essere eventualmente conservati per un periodo comunque non superiore a dodici mesi dalla loro registrazione, in riferimento a finalità commerciali, pubblicitarie o di profilazione, perseguite anche da parte di terzi, salva la loro trasformazione in forma anonima che non permetta di identificare gli interessati, anche indirettamente o collegando banche di dati. Eventuali intenzioni di trattare i dati oltre tali termini potranno essere attuate solo previa valutazione di questa Autorità ai sensi dell'art. 17 del Codice. In caso di cessazione del rapporto deve cessare ogni loro utilizzazione per le predette finalità.

Deve essere individuato un termine di conservazione dei dati personali una volta cessato il rapporto anche in relazione ad eventuali finalità amministrative, non superiore ad un trimestre (fatti salvi eventuali specifici obblighi di legge sulla conservazione di documentazione contabile, evitando una loro applicazione impropria). Occorre specificare questi aspetti nell'informativa e predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi ai quali gli stessi siano stati eventualmente comunicati (specie a fini di profilazione o di *marketing*).

I dati personali che rientrano nella nozione di "dati di traffico" possono essere trattati nei soli limiti di legge (artt. 123 e 132 del Codice). Non è consentito accedere ad informazioni archiviate nell'apparecchio terminale dell'abbonato o utente al fine di archiviare informazioni o monitorare le operazioni effettuate (art. 122, comma 1, del Codice).

Infine, laddove uno stesso soggetto (ad esempio, un centro servizi) svolga la propria attività per conto di più fornitori deve essere garantita una separazione nella gestione dei dati personali. In particolare, le eventuali banche di dati costituite non possono essere interconnesse.

7. Ulteriori prescrizioni

Restano fermi, in aggiunta alle prescrizioni del presente provvedimento, gli obblighi che il Codice detta ai titolari del trattamento, obblighi che potranno essere sviluppati attraverso il previsto codice di deontologia e di buona condotta per i servizi di comunicazione elettronica (artt. 122 e 133 del Codice), e la cui inosservanza espone all'inutilizzabilità dei dati trattati (art. 11 del Codice) oltre che alle pertinenti sanzioni amministrative e penali (artt. 161 ss. del Codice).

Ci si riferisce, in particolare:

a) all'obbligo di notificazione al Garante dei trattamenti effettuati
   - con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica, con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti (art. 37, comma 1, lett. *d*), del Codice);
   - con dati sensibili per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie (art. 37, comma 1, lett. *e*), del Codice);
   - con dati idonei a rivelare lo stato di salute e la vita sessuale ai fini di "…*prestazione di servizi sanitari per via telematica* …" (art. 37, comma 1, lett. *b*), del Codice);

b) agli obblighi relativi all'adozione delle misure di sicurezza rapportate alle conoscenze acquisite in base al progresso tecnico (artt. 31-35 e Allegato B) del Codice), anche di tipo "minimo", in particolare per ciò che riguarda la verifica dei profili di autenticazione e autorizzazione, anche al fine di prevenire la fatturazione di servizi non richiesti;

c) alla selezione dei soggetti che, in qualità di incaricati e responsabili del trattamento, sono autorizzati a compiere le operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite, sotto la diretta autorità del fornitore (artt. 29 e 30 del Codice). L'eventuale preposizione di eventuali responsabili ed incaricati "esterni" incontra, nel settore in esame, precisi limiti di legge (art. 123, comma 5, del Codice) e non può portare ad eludere le garanzie di abbonati ed utenti in tema di comunicazione dei dati a terzi, di trasparenza nell'informativa e di rispetto delle finalità dichiarate;

d) all'obbligo di adottare le misure necessarie per agevolare l'esercizio dei diritti degli interessati e il relativo riscontro tempestivo, anche per il tramite degli stessi strumenti interattivi utilizzati per la prestazione dei servizi richiesti (artt. 9, comma 1 e 10, comma 1, del Codice).

8. Informazioni al Garante

Ai sensi e per gli effetti di cui agli artt. 157, 164 e 168 del Codice, i titolari del trattamento indicati negli atti di procedimenti pendenti presso l'Ufficio sono invitati a confermare al Garante, entro e non oltre il 15 maggio 2005, che i trattamenti di dati da essi effettuati sono conformi alle prescrizioni del presente provvedimento, indicando ogni informazione utile al riguardo ed allegando la pertinente documentazione.

TUTTO CIÒ PREMESSO IL GARANTE:

prescrive, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, ai titolari del trattamento dei dati relativi ai servizi televisivi interattivi, le misure necessarie ed opportune indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti.

Roma, 3 febbraio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

41 Disposizioni in materia di comunicazione e di propaganda politica 3 marzo 2005(*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Considerato che il 3 e il 4 aprile e nel mese di maggio 2005 si terranno alcune elezioni amministrative e che nella primavera del 2005 è prevista altresì una consultazione referendaria;

Considerato che candidati e forze politiche intraprendono numerose iniziative di comunicazione e di propaganda e che ciò comporta l'impiego di dati personali per l'inoltro di messaggi elettorali e politici al fine di rappresentare le proprie posizioni in relazione alle elezioni e ai referendum;

Considerato che il diritto riconosciuto a tutti i cittadini di concorrere con metodo democratico a determinare la politica nazionale (art. 49 Cost.) deve essere esercitato nel rispetto dei diritti e delle libertà fondamentali delle persone cui si riferiscono le informazioni utilizzate e, in particolare, del diritto fondamentale alla protezione dei dati personali (art. 1 del Codice);

Visto l'art. 13, comma 4, del Codice ai sensi del quale, se i dati non sono raccolti presso la persona cui si riferiscono, l'informativa di cui al comma 1 del medesimo articolo è fornita all'interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione;

Considerato che, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, il Garante ha il compito di dichiarare se l'adempimento da parte di un determinato titolare del trattamento all'obbligo di informativa comporta o meno un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato, e di prescrivere in tal caso eventuali misure appropriate;

Visto il provvedimento generale di questa Autorità del 12 febbraio 2004[1] (pubblicato sulla *Gazzetta Ufficiale* 24 febbraio 2004, n. 45, allegato al presente provvedimento e le cui prescrizioni si intendono qui integralmente richiamate), con il quale sono stati indicati i presupposti e le garanzie in base alle quali partiti e movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare lecitamente, a fini di propaganda elettorale, dati personali estratti in particolare da fonti pubbliche;

Considerato che il quadro di garanzie e di adempimenti richiamati con il predetto provvedimento del 12 febbraio 2004 opera anche in relazione alle prossime consultazioni elettorali sopraindicate;

Considerato che, per il solo perseguimento delle iniziative referendarie e per i trattamenti a ciò finalizzati, non è necessaria alcuna manifestazione di consenso ulteriore rispetto alla sottoscrizione delle richieste referendarie, per la cui validità i promotori sono tenuti a raccogliere, per legge, alcuni dati personali dei sottoscrittori (artt. 7 e 8 l. 25 maggio 1970, n. 352; art. 24, comma 1, lett. *a*), d.lg. n. 196/2003), e a darne comunicazione

(*) ***G.U.*** **18 marzo 2005, n. 64**
[doc. *web* n. 1107658]

(1) **[doc. *web* n. 634369]**

agli organi preposti alla verifica della regolarità delle richieste (artt. 9 ss. l. 25 maggio 1970, n. 352; art. 24, comma 1, lett. *a*), citato);

Considerato che, invece, coloro che intendono eventualmente trattare i predetti dati per finalità diverse da quelle collegate alla richiesta referendaria devono previamente richiedere un consenso informato, libero, scritto e distinto dalla predetta sottoscrizione delle richieste referendarie;

Considerato che, con il predetto provvedimento, i soggetti che effettuano propaganda elettorale sono stati altresì esonerati temporaneamente, a determinate condizioni, dall'obbligo di fornire previamente l'informativa ai soggetti interessati al trattamento (art. 13 del Codice);

Ritenuto necessario richiamare nel presente provvedimento le garanzie già segnalate dal Garante nel citato provvedimento del 12 febbraio 2004;

Considerata la necessità di esonerare in via temporanea dall'obbligo dell'informativa di cui all'art. 13 del Codice partiti e movimenti politici, comitati promotori, sostenitori e candidati che trattano dati personali per esclusiva finalità di comunicazione politica o di propaganda, nel circoscritto ambito temporale concernente le menzionate tornate di consultazioni elettorali amministrative e referendarie;

Ritenuto che, applicando i principi affermati nel citato provvedimento del 12 febbraio 2004 a proposito dell'obbligo di informativa, deve ritenersi proporzionato rispetto ai diritti degli interessati esonerare il soggetto che utilizza i dati per esclusivi fini di propaganda elettorale dall'obbligo di fornire l'informativa, sino alla data del 30 giugno 2005; ciò, con riferimento all'informativa dovuta a persone cui si riferiscono dati personali estratti da fonti pubbliche accessibili a chiunque, che non siano contattate da chi utilizza i dati o che ricevano materiale di propaganda diverso da lettere articolate o messaggi di posta elettronica, che non permetta l'inserimento dell'informativa;

Ritenuto che, decorsa la data del 30 giugno 2005, partiti e movimenti politici, comitati promotori, sostenitori e candidati possano continuare a trattare (anche mediante mera conservazione) dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità di propaganda elettorale e di connessa comunicazione politica, solo se informeranno gli interessati entro il 30 settembre 2005 nei modi previsti dall'art. 13 del Codice;

Ritenuto che, nel caso in cui partiti e movimenti politici, comitati promotori, sostenitori e candidati non informino gli interessati entro il predetto termine del 30 settembre 2005 nei modi previsti dall'art. 13 del Codice, i dati dovranno essere cancellati o distrutti;

Rilevato che l'interessato può esercitare i diritti di cui all'art. 7 del Codice, con riferimento ai quali il titolare del trattamento è tenuto a fornire un idoneo riscontro;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Giuseppe Santaniello;

TUTTO CIÒ PREMESSO, IL GARANTE:

a) prescrive ai titolari di trattamento interessati, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare le misure necessarie ed opportune richiamate nel presente provvedimento, al fine di rendere il trattamento conforme alle disposizioni vigenti;
b) ai sensi dell'art. 13, comma 5, del Codice dispone che partiti e movimenti politici, comitati promotori, sostenitori e candidati, i quali trattino dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità

41

di propaganda elettorale e di connessa comunicazione politica in occasione delle consultazioni elettorali, amministrative e referendarie del primo semestre del 2005, possano astenersi dall'informare gli interessati alle condizioni e nei limiti indicati in motivazione; c) dispone che il presente provvedimento sia pubblicato sulla *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 3 marzo 2005

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

42 Trattamento dei dati sensibili nella pubblica amministrazione 30 giugno 2005(*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria e il Codice in materia di protezione dei dati personali (direttiva n. 95/46/Ce; d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO:

1. Considerazioni introduttive

Il Codice entrato in vigore il 1° gennaio 2004 ha riunito in modo organico la normativa di tutela relativa al trattamento dei dati personali; ha offerto all'intera amministrazione pubblica un'occasione significativa per portare a compimento il processo di modernizzazione, in modo da adeguare il proprio assetto organizzativo e funzionale dando idonee risposte alle istanze dei cittadini rivolte al massimo rispetto dei diritti e delle libertà fondamentali.

In questo quadro, il Garante rileva, però, con rammarico che numerose amministrazioni pubbliche non hanno dato piena attuazione al Codice.

In particolare, questa Autorità segnala che non sono state ancora introdotte le garanzie previste in ordine al trattamento di alcune informazioni che riguardano profili particolarmente delicati della sfera privata delle persone, ovvero dei *cd.* dati "sensibili".

La vicenda incide in termini rilevanti sulla sfera dei diritti dei cittadini.

L'utilizzo di queste informazioni (concernenti la salute, la vita sessuale, la sfera religiosa, politico-sindacale o filosofica, nonché l'origine razziale ed etnica) è inoltre soggetto a rigorose cautele anche in base alla disciplina comunitaria, la quale vieta il loro trattamento a meno che ricorrano specifici motivi di interesse pubblico rilevante e siano altresì assicurate opportune garanzie (art. 8 direttiva cit.). Analoghe cautele sono previste per i dati di carattere giudiziario. L'inerzia delle pubbliche amministrazioni lede, quindi, non solo il diritto dei cittadini alla protezione dei dati personali, ma comporta anche una violazione del diritto comunitario.

Il ritardo accumulato su questo piano è eccessivo. Sin dal 1997, vigente la legge n. 675/1996, ed anche dopo l'approvazione del Codice nel 2003, i soggetti pubblici hanno infatti potuto avvalersi di un lungo periodo transitorio e di diverse proroghe. L'eventuale protrarsi dell'inerzia delle amministrazioni anche dopo il 31 dicembre 2005 (data di scadenza dell'ultima proroga) risulterebbe del tutto ingiustificata.

L'Autorità esprime viva preoccupazione in relazione al rispetto del termine di legge del 31 dicembre prossimo.

(*) *G.U.* 23 luglio 2005, n. 170
[doc. *web* n. 1144445]

Se non interverranno per tale data i necessari atti di natura regolamentare il trattamento dei dati sensibili e giudiziari dovrà essere infatti interrotto a decorrere dal 1° gennaio prossimo. La prosecuzione del trattamento di dati sensibili e giudiziari dopo tale data concretizzerebbe un illecito, con conseguenti responsabilità di diverso ordine, anche contabile e per danno erariale; potrebbe inoltre comportare l'inutilizzabilità dei dati trattati indebitamente, nonché il possibile intervento di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 3 d.l. 24 giugno 2004, n. 158, come modificato dalla l. 27 luglio 2004, n. 188; art. 11, commi 1, lett. *a*) e 2, del Codice).

Nel quadro della tematica in esame, le amministrazioni pubbliche hanno l'obbligo - accanto ad altri doveri in materia- di rendere trasparenti ai cittadini quali informazioni vengono raccolte tra quelle particolarmente delicate cui si è fatto riferimento; devono altresì chiarire come utilizzano queste informazioni per le finalità di rilevante interesse pubblico individuate con legge. Tali indicazioni vanno trasfuse in un atto regolamentare cui va data ampia pubblicità (artt. 4, comma 1, lett. *d*) ed *e*), 20, comma 2 e 21, comma 2, del Codice).

Non si tratta di un mero adempimento formale, oppure di una semplice ricognizione di prassi esistenti, poiché da tali regolamenti discenderanno effetti sostanziali per i cittadini interessati.

Gli schemi dei regolamenti devono essere sottoposti al Garante per l'espressione del parere, cui i soggetti pubblici devono poi conformarsi.

Considerata l'ampiezza del settore, il Codice prevede anche la possibilità che siano redatti schemi tipo per insiemi omogenei di amministrazioni, sui quali può essere pertanto espresso un unico parere.

Per contribuire alla corretta applicazione del Codice, il Garante ha intensificato la collaborazione finalizzata alla predisposizione di tali schemi tipo con organismi rappresentativi di regioni, autonomie locali ed università, nonché, in riferimento alle rispettive funzioni istituzionali, con la Presidenza del Consiglio dei ministri e il Dipartimento della funzione pubblica.

Il Garante resta però in attesa di ricevere per il parere sia gli schemi tipo eventualmente proposti, sia gli schemi di regolamento predisposti da singole amministrazioni.

2. Aspetti procedurali

Diversi documenti del Garante e più di una circolare evidenziano da tempo la problematica e la circostanza, ribadita dal Codice, che le amministrazioni non possono avvalersi, nel caso di specie, di meri atti che, anche se denominati regolamenti, non hanno, anche per la loro eventuale rilevanza solo interna, la necessaria natura di fonte normativa suscettibile di incidere su diritti e libertà fondamentali di terzi (*Provv.* del 17 gennaio 2002[1], in *Boll.* n. 24, p. 40 e 16 giugno 1999[2], in *Boll.* n. 9, p. 19; *note* del Garante rivolte alla Presidenza del Consiglio dei ministri il 10 settembre 1999[3], il 10 novembre 2000[4] e il 3 maggio 2001[5], in *Boll.* n. 9, p. 31, n. 14-15, p. 26 e n. 20, p. 36).

Spetta ai soggetti pubblici che trattano i dati adottare l'atto di natura regolamentare, o avvalendosi dei poteri ad essi riconosciuti dall'ordinamento di riferimento, oppure promuovendo l'adozione di un regolamento da parte della competente amministrazione di riferimento la quale eserciti, ad esempio, poteri di indirizzo e controllo (*es.*: artt. 4 e 14 d.lg 30 marzo 2001 n. 165 e, a titolo esemplificativo, artt. 8 e ss. d.lg. 30 luglio 1999, n. 300 e 9 d.lg. 29 ottobre 1999, n. 419).

Gli atti di natura regolamentare da adottare devono essere predisposti previa ricognizione attenta dei trattamenti di dati sensibili e giudiziari in fase di attuale trattamento o che si intende trattare in futuro.

Occorre poi tenere presente che potranno essere prese in considerazione nei regolamenti le sole finalità di rilevante interesse pubblico già individuate specificamente dal Codice o,

(1) [doc. *web* n. 1064681]

(2) [doc. *web* n. 42312]

(3) [doc. *web* n. 1091923]

(4) [doc. *web* n. 1087943]

(5) [doc. *web* n. 1076053]

come quest'ultimo prevede, da un'espressa previsione di legge che, anche se collocata fuori del Codice, le evidenzi comunque puntualmente nei termini richiesti (art. 20 e Parte II del Codice).

La ricognizione, che presuppone il necessario coinvolgimento delle articolazioni interne del soggetto pubblico interessato, permette a quest'ultimo di effettuare anche un'ulteriore verifica circa la rispondenza dei trattamenti in corso con i principi del Codice oggi già direttamente applicabili (e ovviamente da rispettare anche in sede regolamentare), nonché di adeguare prontamente procedure in atto eventualmente non conformi a legge (principio di indispensabilità in rapporto alle finalità perseguite; verifiche periodiche dei vari requisiti dei dati –esattezza, aggiornamento, pertinenza, completezza, ecc.– e del loro rapporto con gli adempimenti da svolgere; scelta di modalità volte a prevenire violazioni di diritti e libertà fondamentali; raccolta dei dati sensibili e giudiziari di regola presso gli interessati; particolari cautele rispetto a dati riferiti a terzi non direttamente interessati ai compiti o adempimenti da svolgere; divieto di diffusione di dati sulla salute ecc.: *cfr.* art. 22 del Codice).

3. Il parere del Garante

Gli atti di natura regolamentare devono essere adottati, in ogni caso, in conformità al parere del Garante. Come accennato, il parere può essere espresso anche su schemi tipo, il che contribuisce a rendere più organiche le garanzie in riferimento ad altre amministrazioni e semplifica, inoltre, l'iter di approvazione degli atti.

Infatti, una volta espresso dal Garante il parere su uno schema tipo riguardante l'attività di soggetti pubblici che svolgono attività omogenee, lo schema di ciascun regolamento non deve essere sottoposto singolarmente a questa Autorità, sempreché il trattamento ipotizzato sia attinente e conforme allo schema tipo esaminato.

É invece necessario sottoporre al Garante uno schema di regolamento per uno specifico parere solo se:

a) manca uno schema tipo già esaminato dall'Autorità;
b) vi è uno schema tipo al quale l'amministrazione deve apportare modifiche sostanziali o integrazioni non formali che riguardano (a causa di ulteriori categorie di dati o di altre rilevanti operazioni di trattamento) casi in esso non considerati nello schema tipo.

Anche in questi due casi, il Garante è impegnato ad esprimere il parere nel termine di 45 gg. dal ricevimento della richiesta (o nei 20 gg. dal ricevimento degli elementi istruttori ricevuti dalle amministrazioni interessate), decorsi i quali, se non interviene un parere formale, il soggetto può adottare comunque il regolamento e proseguire poi il trattamento (art. 154, comma 5, del Codice).

4. Contenuto dell'atto regolamentare e pubblicità

In questa sede, Il Garante intende fornire alle amministrazioni che non potranno avvalersi di schemi tipo alcune prescrizioni di carattere generale per contribuire all'adozione di adeguate bozze di regolamento più attente ai profili sostanziali di tutela, più comprensibili da parte dei cittadini e non basate su approcci meramente formali alla tematica.

Questa particolare attenzione è ancor più necessaria se si tiene conto che, dal 1° gennaio 2006 non sarà lecito alcun trattamento dei dati sensibili e giudiziari che non sia disciplinato espressamente nei regolamenti.

Lo schema di regolamento deve contenere sinteticamente, ma in termini adeguati ed agevolmente comprensibili, le seguenti indicazioni specificate per categorie.

Dati indispensabili

Occorre individuare le tipologie di informazioni sensibili e giudiziarie che si devono necessariamente utilizzare in rapporto alle attività istituzionali svolte, avendo cura che a ciascun adempimento corrisponda il trattamento delle sole informazioni per ciò strettamente

42

indispensabili (art. 22, comma 3, del Codice). I dati vanno indicati solo per tipologie, evitando elencazioni eccessivamente sommarie.

Operazioni di trattamento indispensabili

Vanno parimenti individuate le operazioni che si devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico puntualmente individuate per legge, mettendo in particolare evidenza le operazioni che possono spiegare effetti maggiormente significativi per l'interessato e per le quali sono pertanto necessarie più garanzie. Anche in questo caso la descrizione è per tipologie, evitando indicazioni del tutto generiche circa l'impiego delle informazioni.

Tra tali operazioni rientrano, in particolare, quelle svolte pressoché interamente mediante siti web, o volte a definire in forma completamente automatizzata profili o personalità di interessati, le interconnessioni e i raffronti tra banche di dati gestite da diversi titolari, oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento (art. 22, c. 9, 10 e 11, del Codice), nonché la comunicazione dei dati a terzi.

Si possono invece indicare più sinteticamente le operazioni "ordinarie" e più ricorrenti di trattamento (raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione ecc.).

Ulteriore contenuto dello schema di regolamento

É opportuno che il soggetto pubblico descriva sinteticamente, in termini comunicativi, anche la complessiva attività svolta, con particolare riguardo agli aspetti più incisivi per i diritti dei cittadini.

Non è quindi necessario scendere in eccessivi livelli di dettaglio non richiesti dal Codice; né è richiesta la riproduzione analitica delle disposizioni del Codice (in particolare, degli artt. 3, 11, 18-22, 85 s. e 95 s.).

Andrebbe altresì evitato di disciplinare situazioni già adeguatamente regolate sul piano legislativo e regolamentare quanto ai tipi di dati e di operazioni, come avviene nel caso dei dati personali trattati per effetto di un accesso a documenti amministrativi (artt. 59 e 60 del Codice; l. n. 241/1990 e successive modificazioni ed integrazioni).

Va inoltre rilevato in questa sede che la normativa sugli obblighi e compiti che rendono indispensabile utilizzare dati sensibili e giudiziari deve essere oggetto di un espresso riferimento nell'informativa da rendere agli interessati (art. 22, comma 2, del Codice). L'indicazione di tale normativa può essere quindi utile anche nell'ambito dello schema tipo, contribuendo ad evitare che il regolamento prenda erroneamente in considerazione attività che, pur essendo demandate al soggetto pubblico, non rientrano tra quelle che una fonte primaria non ha ritenuto di importanza tale da legittimare il trattamento di dati sensibili e giudiziari, in quanto non considerate "rilevanti finalità di interesse pubblico".

Da ultimo, tra le garanzie individuate dal Codice figura il diritto dei cittadini di conoscere con quali modalità sono utilizzate le predette informazioni che lo riguardano (art. 20, comma 2, del Codice).

Va pertanto prescritto ai soggetti pubblici interessati di intraprendere, in aggiunta alla pubblicità legale da assicurare agli atti regolamentari secondo i singoli ordinamenti, adeguate iniziative per assicurare idonea conoscibilità alle scelte adottate a proposito dei dati sensibili e giudiziari, utilizzando non solo i siti web istituzionali, ma anche le iniziative di comunicazione istituzionale cui essi sono tenuti.

Riservandosi di concludere rapidamente in separata sede i processi di collaborazione già avviati con alcuni organismi rappresentativi di soggetti pubblici, il Garante ritiene infine doveroso prescrivere in questa sede a tutti i soggetti pubblici interessati di adottare le predette misure, necessarie o, a seconda dei casi, opportune.

A tal fine, il Garante pone anche a disposizione dei soggetti pubblici, in allegato al pre-

sente provvedimento, un modello di riferimento per redigere gli schemi. Questo modello aggiorna quello già predisposto dal Garante il 17 gennaio 2002.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari di trattamenti di dati personali oggetto del presente provvedimento di adottare le misure necessarie ed opportune ivi indicate al fine di rendere i trattamenti medesimi conformi alle disposizioni vigenti;
b) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale*, ai sensi dell'art. 143, comma 2, del Codice.

Roma, 30 giugno 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

Art. ...
1. Il presente regolamento, in attuazione del Codice in materia di protezione dei dati personali (artt. 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196), identifica le tipologie di dati sensibili e di operazioni indispensabili a ... per perseguire le finalità di rilevante interesse pubblico espressamente individuate da apposita previsione di legge.

Art. ...
1. Ai sensi dell'art. 1, ... , per le finalità di ... tratta le seguenti tipologie di dati sensibili e giudiziari mediante i tipi di operazioni di seguito indicati.

INDICAZIONE DEL TRATTAMENTO E DESCRIZIONE RIASSUNTIVA DEL CONTESTO

Indicare sinteticamente il contesto in cui il trattamento è effettuato (*es.*: gestione del rapporto di lavoro del personale), descrivendo anche, con linguaggio chiaro e comunicativo, le caratteristiche principali del trattamento e del flusso informativo

FINALITÀ DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE

Indicare le finalità di rilevante interesse pubblico specificamente indicate dal Codice o da una norma di legge e il relativo riferimento normativo (*es.*, instaurare e gestire il rapporto di lavoro di qualunque tipo con il personale dipendente, anche a tempo parziale o temporaneo, nonché altre forme di lavoro non subordinato).

FONTE NORMATIVA

Indicare, se possibile, le fonti normative sull'attività istituzionale cui il trattamento è collegato (*es.*: artt. 2094-2134 del codice civile); legge n. 300/1970; d.lg. n. 165/2001; d.lg. n. 151/2001).

42

TIPI DI DATI TRATTATI *(barrare le caselle corrispondenti)*

❑ origine	❍ razziale	❍ etnica	
❑ convinzioni	❍ religiose	❍ filosofiche	❍ d'altro genere
❑ convinzioni	❍ politiche	❍ sindacali	
❑ stato di salute	❍ patologie attuali	❍ patologie pregresse	
	❍ terapie in corso	❍ anamnesi familiare	

❑ vita sessuale

❑ dati di carattere giudiziario (art. 4, comma1, lett. *e*), del Codice)?

OPERAZIONE ESEGUITE *(barrare le caselle corrispondenti)*

Particolari forme di trattamento

❑ Interconnessioni e raffronti di dati:

❍ con altre informazioni o banche dati dello stesso soggetto pubblico (*specificare quali ed indicarne i motivi*): ...

❍ con altri soggetti pubblici o privati (*specificare quali ed indicare la base normativa*): ...

❑ Trattamento automatizzato volto a definire il profilo o la personalità dell'interessato ai fini dell'adozione di un provvedimento amministrativo o giudiziario (*specificare quali ed indicarne i motivi o la base normativa*): ...

❑ Comunicazione ai seguenti soggetti per le seguenti finalità (i*ndicare l'eventuale base normativa*): ...

❑ Diffusione (*specificare l'ambito ed indicare l'eventuale base normativa*): ...

❑ Altre operazioni (*indicare eventuali altre operazioni effettuate sui dati, diverse da quelle sopra indicate*): ...

Altre tipologie più ricorrenti di trattamento

❑ Raccolta:	❍ presso gli interessati	❍ presso terzi
❑ Elaborazione:	❍ in forma cartacea	❍ con modalità informatizzate

Altre operazioni indispensabili rispetto alla finalità del trattamento e diverse da quelle "ordinarie" quali la registrazione, la conservazione, la cancellazione o il blocco nei casi previsti dalla legge (*specificare*): ...

43 Sicurezza presso il C.e.d. del Dipartimento della pubblica sicurezza 7 luglio 2005 (*)

Registro delle deliberazioni
n. 16 del 7 luglio 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria e il Codice in materia di protezione dei dati personali (direttiva n. 95/46/Ce; d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

Premesso che ai trattamenti di dati personali effettuati in riferimento al Centro elaborazione dati (C.e.d.) del Dipartimento della pubblica sicurezza del Ministero dell'interno, di cui all'articolo 8 della legge 1° aprile 1981, n. 121, e successive modificazioni, si applicano le disposizioni del Codice in materia di protezione dei dati personali, anche in relazione alle misure di sicurezza da adottare (artt. 3, 11, 31, 33, 53 ss. del Codice);

Considerato che le disposizioni del Codice attuano anche la Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali, applicabile anche ai trattamenti sopra descritti, e della Raccomandazione R(87)15 del Consiglio d'Europa volta a disciplinare l'utilizzo dei dati a carattere personale nel settore della polizia, adottata il 17 settembre 1987, e che in base alla Dichiarazione relativa alla protezione dei dati firmata a margine dell'Accordo di Schengen il Governo italiano ha assunto il formale impegno ad introdurre le disposizioni nazionali necessarie ad assicurare, nel predetto settore, un livello di protezione dei dati almeno uguale a quello indicato nei predetti atti internazionali, per poter applicare il predetto Accordo e la relativa Convenzione di applicazione;

Considerato che le vigenti disposizioni concernenti le procedure di raccolta, di accesso, di comunicazione e di correzione dei dati registrati nel predetto C.e.d., nonché le relative misure di sicurezza contenute nel regolamento approvato con d.P.R. 3 maggio 1982, n. 378, devono essere rese pienamente conformi ai principi e alle regole del Codice, in particolare per quanto riguarda l'aggiornamento dei dati, la loro conservazione e gli standard di sicurezza;

Considerato che l'articolo 57 del Codice prevede che, con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, devono essere individuate le modalità di attuazione dei principi del Codice in relazione al trattamento dei dati effettuato dal predetto C.e.d., anche al fine di integrare e modificare il predetto d.P.R. 3 maggio 1982 n. 378, in attuazione della citata Raccomandazione R(87)15 del Consiglio d'Europa, anche sotto il profilo dell'aggiornamento e dell'efficacia delle misure di sicurezza;

(*) [doc. *web* n. 1170253]

43

Ritenuto di dover, allo stato, prescrivere al Ministero dell'interno, ai sensi dell'articolo 154, comma 1, lett. *c*), del Codice, di adottare ogni opportuna misura volta ad incrementare i livelli di sicurezza nel trattamento dei dati, anche mediante accelerazione dell'iter per l'adozione, su proposta del medesimo Ministero, del predetto regolamento previsto dall'articolo 57 del Codice;

TUTTO CIÒ PREMESSO E CONSIDERATO IL GARANTE:

ai sensi dell'articolo 154, comma 1, lett. *c*), del Codice prescrive al Ministero dell'interno di adottare ogni opportuna misura volta ad incrementare i livelli di sicurezza nel trattamento dei dati, anche mediante accelerazione dell'iter per l'adozione del regolamento previsto dall'articolo 57 del Codice.

Roma, 7 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

44 Elenchi telefonici: semplificate le procedure per i "categorici" 14 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan, del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 129, comma 2, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) che, in attuazione della disciplina comunitaria e in particolare della direttiva comunitaria n. 2002/58/Ce, ha individuato nella "mera ricerca dell'abbonato per comunicazioni interpersonali" la finalità primaria degli elenchi telefonici;

Visto il provvedimento del 23 maggio 2002[1] e del 15 luglio 2004[2] con il quale questa Autorità ha segnalato e prescritto a tutti gli operatori le garanzie necessarie per trattare dati personali al fine di formare i nuovi elenchi telefonici e prestare i servizi di informazione all'utenza;

Viste le note pervenute da vari soggetti che intendono pubblicare elenchi telefonici organizzati per categorie merceologiche/professionali (*cd.* elenchi "categorici"), con le quali è stato chiesto al Garante di fornire un chiarimento in ordine all'applicabilità o meno a tali elenchi categorici della disciplina contenuta nell'art. 129 del Codice, nonché delle prescrizioni riportate nei predetti provvedimenti dell'Autorità del 23 maggio 2002 e del 15 luglio 2004;

Considerata la particolare complessità ed onerosità delle procedure necessarie per adempiere all'obbligo di informativa (art. 13 del Codice) in relazione ai dati raccolti presso terzi concernenti tutti gli interessati che verranno inseriti negli elenchi *cd.* categorici, e rilevato che l'informativa resa in questo caso secondo le ordinarie modalità comporterebbe un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato (art. 13, comma 5, lett. *c*), del Codice), visto anche il numero particolarmente elevato di interessati, in particolare di soggetti imprenditoriali e di liberi rofessionisti, che dovrebbero essere altrimenti informati singolarmente;

Ritenuta la necessità di prescrivere ai titolari del trattamento interessati in quanto editori di elenchi categorici, ai sensi degli artt. 154, comma 1, lett. *c*) e 13, commi 4 e 5, lett. *c*) del Codice, le misure che devono essere da essi adottate con particolare riferimento, rispettivamente, alle modalità di acquisizione ed inserimento dei dati personali e all'informativa;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

PREMESSO CHE:

- gli elenchi "categorici" hanno carattere commerciale e promozionale, contenendo varie informazioni relative allo svolgimento delle attività economiche ed equiparate dei soggetti interessati, in particolare aziende, professionisti, esercizi commerciali ed enti;
- le specifiche finalità di tali elenchi non sono interamente riconducibili a quelle degli elenchi "alfabetici" del servizio universale contenenti i dati degli abbonati ai servizi di telefonia fissa e mobile, il cui scopo, secondo quanto previsto dalla nuova disciplina in fase di attuazione, è invece quello di consentire la "mera ricerca del-

(*) [doc. *web* n. 1151640]

(1) [doc. *web* n. 1032397]

(2) [doc. *web* n. 1032381]

44

l'abbonato per comunicazioni interpersonali" (art. 129, comma 2, del Codice);
- agli elenchi "categorici" non si applicano, quindi, le prescrizioni contenute nel provvedimento adottato dal Garante il 15 luglio 2004 ai sensi dell'art. 129 del Codice, e che per la loro formazione i soggetti che trattano i dati destinati a figurare nei medesimi elenchi possono utilmente applicare, in conformità alle prescrizioni di legge, la previsione di carattere generale che permette di prescindere dal consenso dei soggetti interessati in quanto il trattamento "riguarda dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d*), del Codice);
- la pubblicazione degli elenchi "categorici" deve comunque rispettare gli altri obblighi e diritti in materia di protezione dei dati personali;
- tale rispetto deve riguardare anche: a) la necessaria completezza dei dati relativi ad interessati compresi nelle categorie che verranno riportate, a seconda dei casi, nelle distinte tipologie di elenchi pubblicati; b) la necessità che gli elenchi "categorici", ove formati attingendo alla base di dati unica di cui all'allegato II del predetto provvedimento del 15 luglio 2004, non comprendano gli estremi identificativi di soggetti che abbiano eventualmente chiesto di non figurare nei predetti elenchi "alfabetici" (essendosi anche avvalsi del modello di informativa di cui all'allegato IV del medesimo provvedimento o, comunque, in altra forma), fermo restando che tale esclusione non fa venir meno il predetto requisito della completezza;
- l'art. 13, comma 5, del Codice prevede che il Garante, con esclusivo riferimento al caso in cui i dati siano raccolti presso terzi, anziché presso i diretti interessati, può disporre l'"esonero" in tutto o in parte dall'obbligo dell'informativa o altra soluzione equipollente, qualora l'informativa con modalità ordinarie comporterebbe un impiego di mezzi che il Garante dichiari manifestamente sproporzionato rispetto al diritto tutelato; rilevato che tale manifesta sproporzione può essere ravvisata dal Garante sia caso per caso, sia, come rilevato con deliberazione del 26 novembre 1998[1] (pubblicata nel *Bollettino* ufficiale del Garante "Cittadini e Società dell'Informazione", 1998, anno II, n. 6, p. 81), "in riferimento a settori o tipi di trattamento";
- ritenuto che, in base agli atti acquisiti, la singola informativa da parte di ciascun titolare comporterebbe un impiego di mezzi sproporzionato rispetto al diritto tutelato (art. 13, comma 5, del Codice), stanti, nel caso di specie, le varie operazioni di distinti soggetti che dovrebbero effettuare, con riferimento a più interessati, informative aventi caratteristiche omogenee;
- è tuttavia necessario assicurare un'informativa generale comunque adeguata, prescrivendo in questa sede ai soggetti interessati una misura appropriata ai sensi del medesimo art. 13, comma 5, consistente nelle informative di cui al seguente dispositivo;

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari del trattamento di dati personali connessi all'edizione e pubblicazione di elenchi categorici di conformare il medesimo trattamento agli obblighi e ai diritti richiamati in motivazione, in particolare per quanto riguarda: 1) la necessaria completezza dei dati relativi ad interessati compresi nelle categorie che verranno riportate, a seconda dei casi, nelle distinte tipologie di elenchi pubblicati; 2) la necessità che gli elenchi "categorici", ove formati attingendo alla base di dati unica di cui all'allegato II del predetto provvedimento del 15 luglio 2004, non comprendano gli estremi identificativi di soggetti che abbiano eventualmente chiesto di non figurare nei predetti elenchi "alfabetici", essendosi anche avvalsi del modello di informativa di cui all'allegato IV del medesimo provvedimento o, comunque, in altra forma;
b) ai sensi dell'art. 13, commi 4 e 5, lett. *c*), del Codice autorizza ciascun titolare del trattamento di dati personali connessi all'edizione e pubblicazione di elenchi categorici, in relazione al caso in cui i dati personali siano raccolti non dall'interessato, ma presso terzi, anche in caso di estrazione dei dati dalla base di dati unica di cui all'allegato II al provvedimento del Garante del 15 luglio 2004, ad effettuare l'informativa prevista dal medesimo art. 13, comma 1, mediante pubblicazione di almeno un avviso da pubblicarsi, a

(1) [doc. *web* n. 39624]

cura di ciascun titolare, nei mesi di settembre e ottobre 2005, su almeno tre quotidiani ad ampia diffusione nazionale e con dimensioni non inferiori a 1/4 di pagina, con tenore e modalità che la rendano facilmente leggibile. L'informativa -da trasmettere a questa Autorità allegando copia dell'inserzione- dovrà altresì figurare in una chiara avvertenza inserita, con evidenza, nella parte iniziale dell'elenco categorico cartaceo, oppure pubblicato con modalità elettroniche. In entrambi i casi, l'informativa dovrà comprendere, oltre che agli elementi indicati all'art. 13 del Codice, un riferimento alla disciplina applicabile agli elenchi categorici, nonché alle peculiari garanzie operanti, anche per gli elenchi categorici, in caso di comunicazioni di carattere commerciale nei modi di cui all'art. 130 del Codice (uso di sistemi automatizzati di chiamata; posta elettronica; *telefax*, messaggi del tipo *Mms* o *Sms* o di altro tipo).

Roma, 14 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

45 Ricette mediche, tessera sanitaria e monitoraggio della spesa 21 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la richiesta di parere del Ministro dell'economia e delle finanze;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali e, in particolare, la direttiva n. 95/46/Ce del 24 ottobre 1995;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visto l'articolo 50, comma 10, del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, in materia di monitoraggio della spesa nel settore sanitario;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO:

Nel quadro della problematica riguardante il monitoraggio della spesa sanitaria lo schema di decreto in esame, trasmesso dal Ministro dell'economia e delle finanze per il prescritto parere, concerne il particolare profilo dell'approvazione del protocollo riguardante i dati rilevati dalle ricette mediche (e comunicati, per il tramite del medesimo Ministero, al Ministero della salute e alle regioni), nonché le modalità della loro trasmissione.

OSSERVA:

Lo schema precisa, nel preambolo, che i dati in questione, utilizzati dal Ministero dell'economia e delle finanze ai soli fini di liquidazione provvisoria dei rimborsi dovuti alle strutture di erogazione dei servizi sanitari, possono essere trattati dal medesimo Ministero "per scopi statistici ed altri compiti istituzionali solo in forma anonima, eliminato ogni riferimento ad informazioni che rendono identificabili gli interessati, come il codice fiscale, il codice a barre della tessera sanitaria e il numero progressivo regionale delle ricette".

In coerenza con tale precisazione, lo schema aggiornato di decreto prevede che i dati trasmessi dal Ministero dell'economia e delle finanze al Ministero della salute, all'Agenzia italiana del farmaco (Aifa) e alle regioni abbiano le stesse caratteristiche di anonimato di quelli detenuti e comunicati dal medesimo Ministero (dati anonimi, privi di ogni riferimento ad informazioni che rendono identificabili gli interessati, quali il codice fiscale e il codice a barre della tessera sanitaria).

Conseguenti precisazioni sono state opportunamente apportate nel disciplinare tecnico allegato allo schema di decreto.

(*) [doc. *web* n. 1151167]

Le previsioni dello schema di decreto risultano in linea con le finalità statistiche dell'utilizzo di tali dati da parte delle amministrazioni destinatarie della comunicazione del Ministero dell'economia e delle finanze, fermo restando che le aziende sanitarie locali e le altre strutture sanitarie autorizzate potranno utilizzare le informazioni per lo svolgimento, in conformità alla legge, delle proprie attività istituzionali, ivi compresa la verifica di appropriatezza delle prescrizioni sanitarie.

Ciò premesso, il Garante esprime parere favorevole sullo schema di decreto.

TUTTO CIÒ PREMESSO IL GARANTE:

esprime parere favorevole sullo schema di decreto.

Roma, 21 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

46 Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro 21 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Landini S.p.A. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa al trattamento di dati personali biometrici al fine di verificare le presenze sul luogo di lavoro dei dipendenti;

Visti gli elementi acquisiti a seguito degli accertamenti avviati ai sensi dell'art. 154, comma 1, lettere a), del Codice;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO:

1. Trattamento di dati personali biometrici nel rapporto di lavoro con finalità di verifica della presenza dei dipendenti

Landini S.p.A., industria di coperture in fibrocemento e metalliche che occupa circa trecento dipendenti, ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici dei propri dipendenti finalizzato ad accertarne la presenza sul luogo di lavoro e commisurare, così, la retribuzione ordinaria e straordinaria da corrispondere.

Il funzionamento di questo sistema presuppone una fase di raccolta di dati biometrici (*cd. enrollment*) nella quale la società, avvalendosi di apparecchiature elettroniche dotate di lettore di impronte digitali e di apposito *software*, trasformerebbe l'immagine di una porzione dell'impronta digitale dei lavoratori in un codice numerico, associandolo a ciascun lavoratore con la sua memorizzazione nel sistema informativo aziendale (senza sottoporlo a cifratura o ad altre tecniche equivalenti). Tale codice verrebbe utilizzato quale termine di paragone dei codici numerici ricavati dalla lettura delle (parti di) impronte digitali dei lavoratori, rilevate, in occasione di ciascun ingresso e uscita dal luogo di lavoro, attraverso lettori dislocati in diverse aree dell'azienda e connessi al relativo sistema informativo.

Il trattamento dei dati biometrici non perseguirebbe altra finalità che quella ora descritta. Stando alle dichiarazioni rese dalla società titolare del trattamento (e dal produttore del sistema), una volta terminata la fase di enrollment, non vi sarebbe ulteriore memorizzazione dell'impronta digitale. Ad avviso della società, non sarebbe possibile, inoltre, risalire all'impronta stessa a partire dal codice numerico generato.

Il trattamento di dati biometrici viene giustificato dall'esigenza di prevenire alcune condotte, anche abusive, da parte di alcuni dipendenti (consistenti nello scambio dei *badge*) e lo smarrimento delle tessere magnetiche attualmente in uso; viene quindi ritenuto che il trattamento dei dati biometrici consentirebbe di ovviare a tali inconvenienti, assicurando un grado elevato di certezza nell'identificazione dei lavoratori.

(*) [doc. *web* nn. 1150679, vers. EN 1166892]

Stando alle dichiarazioni rese, verrebbe comunque assicurato ai lavoratori che siano impossibilitati a partecipare all'enrollment (in ragione delle proprie caratteristiche fisiche) o che non intendano acconsentire al trattamento, di attestare la propria presenza sul luogo di lavoro mediante l'apposizione della propria sottoscrizione in un registro delle presenze ubicato presso l'ufficio del personale con riconoscimento "a vista" o, ancora, ricorrendo ad altri "sistemi convenzionali".

2. Trattamento di dati biometrici e applicabilità della disciplina di protezione dei dati personali

Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali.

I dati biometrici che verrebbero rilevati nel caso di specie (porzione dell'impronta digitale) sono informazioni ricavate dalle caratteristiche fisiche di interessati che si vorrebbero identificare in modo univoco, mediante un modello di riferimento (*template*). Quest'ultimo consiste nell'insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

Sia le impronte dattiloscopiche (*cfr. Provv.* Garante 19 novembre 1999[1], in *Boll.* n. 10, p. 68), ancorché raccolte in modo parziale e solo ai fini del completamento della fase dell'enrollment, sia i codici numerici successivamente utilizzati per le descritte operazioni di confronto, in quanto informazioni riferibili ai singoli lavoratori, sono dati personali (art. 4, comma 1, lett. *b*), del Codice). Ne discende, pertanto, l'applicazione della disciplina contenuta nel Codice, così nella fase dell'enrollment, come pure in relazione alle successive operazioni di confronto (con il correlato tracciamento degli orari di ingresso/uscita dal luogo di lavoro).

3. Qualità dei dati, misure di sicurezza e informativa rispetto al trattamento dei dati biometrici

Con riguardo al principio di qualità dei dati, dall'istruttoria svolta emergono perplessità in ordine al corretto funzionamento del sistema che si intende installare.

Allo stato, non risultano documentati i presupposti per un elevato grado di affidabilità del sistema medesimo, tanto che è stata programmata una fase di prova per testarne l'affidabilità. La società non è inoltre in grado, al momento, di indicare il livello della sua accuratezza ricorrendo ai parametri tecnici idonei ad individuare i "falsi negativi" (Frr-*False Rejection Rate*) e i "falsi positivi" (Far-*False Acception Rate*). I sistemi di rilevazione di dati come quelli in esame devono invece offrire una rigorosa garanzia di affidabilità ed integrità dei dati, anche sulla base di certificazioni od omologazioni dei dispositivi che tengano eventualmente conto delle valutazioni di comitati tecnici indipendenti.

Inoltre, dagli elementi forniti non è possibile ricavare con certezza se siano adeguate le misure di sicurezza predisposte a protezione della rete di comunicazione elettronica sulla quale i dati biometrici sono trasmessi dai singoli lettori al sistema centralizzato di acquisizione dati. A tale proposito, una misura opportuna da parte del titolare del trattamento consisterebbe ad esempio nell'utilizzo di chiavi di cifratura dei dati biometrici, indicato anche a livello europeo (*v.*, *ad es.*, il *Documento di lavoro sulla biometria* del Gruppo per la tutela dei dati personali di cui all'art. 29 della direttiva n. 95/46/Ce del 1° Agosto 2003 (punto 3.6), in *http://europa.eu.int/...pdf*).

Anche l'informativa predisposta non risulta adeguata rispetto al trattamento che si intende porre in essere: come detto, dalle dichiarazioni acquisite emerge che, i lavoratori sarebbero liberi di aderire o meno al sistema di rilevazione delle presenze basato sull'utilizzo di dati biometrici; strumenti alternativi sarebbero previsti anche per i lavoratori impossibilitati, per ragioni fisiche, a registrare le presenze mediante l'impiego del sistema bometrico.

(1) [doc. *web* n. 42058]

Tali dichiarazioni, però, non trovano conferma nell'informativa predisposta per gli interessati, secondo la quale il conferimento dei dati, ivi compresi i dati biometrici (espressamente richiamati sotto la voce *"ulteriori specificazioni particolari"*), avrebbe natura obbligatoria. Ciò, ha rilievo anche per la circostanza che il sistema potrebbe operare (con riguardo all'enrollment e ai successivi accessi nei luoghi di lavoro) solo con l'attiva collaborazione personale dei lavoratori interessati, i quali dovrebbero rendersi così disponibili –in assenza di una disposizione di legge che lo imponga ed impregiudicati i profili eventualmente connessi al coinvolgimento delle rappresentanze sindacali– a sottoporre una parte del proprio corpo alle operazioni necessarie per la rilevazione biometrica.

Manca, inoltre, nell'informativa ogni riferimento a tecniche alternative per la rilevazione delle presenze, contravvenendosi, così, all'art. 13 del Codice secondo il quale è necessario che le informazioni da rendere agli interessati enuncino chiaramente tutte le modalità impiegate nel trattamento e la tipologia di dati personali utilizzati per ciascuna di esse.

4. Dati biometrici e principi di protezione dei dati personali: finalità, necessità e pertinenza

Se le ragioni illustrate denotano più di un rilievo in ordine al sistema di rilevazione in esame, la sua liceità deve essere verificata altresì, sotto altri profili concernenti i principi di necessità, proporzionalità, finalità e correttezza, nonché di qualità dei dati (artt. 3 e 11 del Codice; art. 6, direttiva n. 95/46/Ce).

A questo proposito, se pure rientra tra le legittime facoltà del datore di lavoro sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 c.c.) verificando le presenze dei dipendenti e il rispetto dell'orario di lavoro anche ai fini del calcolo della retribuzione, ad esempio attraverso badge, non risulta documentato che il trattamento di dati biometrici in esame (con particolare riguardo all'impronta digitale) sia conforme ai principi di necessità e proporzionalità.

L'utilizzo di tali dati in luoghi di lavoro può essere giustificato in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati (ad esempio, accessi a particolari aree dell'azienda per le quali debbano essere adottati livelli di sicurezza particolarmente elevati in ragione di specifiche circostanze o attività ivi svolte), oppure per finalità di sicurezza del trattamento di dati personali (*v.* Allegato B) al Codice).

Non può invece ritenersi lecito un uso generalizzato e incontrollato dei medesimi dati, specie se si tratta di impronte digitali per le quali occorre anche prevenire eventuali utilizzi impropri e possibili abusi.

Considerata l'utilizzabilità di idonee modalità alternative per un accertamento parimenti rigoroso dell'identità personale, ma meno problematiche per la dignità stessa dei lavoratori interessati (art. 2 del Codice, modalità di cui non è stata rappresentata l'inefficacia nel caso di specie), l'illustrata finalità di computo dell'orario di lavoro in un'azienda come quella istante non risulta, dagli atti, legittimare la rilevazione di impronte digitali le quali sono comunque associate, contrariamente a quanto rilevato dall'istante, ai relativi interessati.

Al di là dei controlli ordinari e a campione circa la presenza dei lavoratori alle uscite e nei luoghi di lavoro, peraltro di agevole accertamento, non è stata dimostrata l'inefficacia, nel caso di specie, di misure che (senza ricorrere al trattamento di dati biometrici, nel rispetto dell'art. 3 del Codice) possono comunque contenere significativamente il rischio di pratiche abusive.

Il titolare del trattamento, per verificare la puntuale osservanza dell'orario di lavoro da parte dei lavoratori, impedendo in pari tempo condotte abusive dei medesimi, può disporre di altri sistemi meno invasivi della sfera personale, della libertà individuale e che non coinvolgano il corpo del lavoratore –aspetti entrambi costitutivi della dignità personale, a presidio della quale sono dettate le discipline di protezione dei dati personali (art. 2 del Codice)–.

Il trattamento in esame deve ritenersi sproporzionato anche in considerazione delle

modalità tecniche prefigurate (centralizzazione dei codici identificativi derivati dall'esame del dato biometrico), ben potendosi adottare, anche da questo punto di vista, misure tecnologiche meno invasive. Infatti, anche a mente della disposizione contenuta nell'art. 3 del Codice, è da ritenere comunque preferibile, laddove sia ammesso il ricorso a dati biometrici, la memorizzazione del codice identificativo su un supporto che resti nell'esclusiva disponibilità dell'interessato (una volta completato il *cd. enrollment*), piuttosto che la registrazione dello stesso a livello centralizzato nel sistema informativo aziendale (con conseguenti più gravi ripercussioni per i diritti individuali in caso di violazione delle misure di sicurezza, di accessi di persone non autorizzate o, comunque, di abuso delle informazioni memorizzate, anche ad opera di terzi).

In conformità con il quadro comunitario (il quale prescrive, non a caso, che i trattamenti di dati che comportano rischi specifici per i diritti e le libertà fondamentali degli interessati, come quello in esame, siano consentiti solo in presenza di una verifica preliminare volta ad appurare la liceità e correttezza del trattamento e ad impartire misure ed accorgimenti a garanzia degli interessati: art. 20 direttiva n. 95/46/Ce; art. 17 del Codice), deve pertanto riscontrarsi l'assenza nel caso di specie nei presupposti di legge per un trattamento di dati corrispondenti ad impronte digitali.

In conclusione, il trattamento oggetto di richiesta non può ritenersi lecito, nei termini di cui in motivazione.

TUTTO CIÒ PREMESSO, IL GARANTE:

ai sensi e per gli effetti di cui agli artt. 3, 11, 17 e 154, comma 1, lett. *d*) del Codice dichiara che il trattamento che Landini S.p.A. intenderebbe effettuare non risulta lecito, nei termini di cui in motivazione, e ne vieta pertanto lo svolgimento se effettuato per le finalità e con le modalità ivi descritte.

Roma, 21 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

47 Portfolio: garanzie nei processi formativi degli alunni 26 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/Ce), anche in relazione agli articoli 2, 10, 11 e 33 della Costituzione;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visto il d.lg. 19 aprile 2004, n. 59 (Definizione delle norme generali relative alla scuola dell'infanzia e al primo ciclo dell'istruzione, a norma dell'art. 1 della l. 28 marzo 2003, n. 53);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

CONSIDERATO:

1. Premessa

La riforma della scuola dell'infanzia e del primo ciclo di istruzione -scuola primaria e scuola secondaria di primo grado- ha introdotto la redazione di un documento di valutazione ed orientamento, denominato "Portfolio (o cartella) delle competenze individuali", da redigere singolarmente per ciascun alunno.

Il Portfolio documenta nei predetti cicli di istruzione i processi formativi degli alunni e ne accompagna in tali ambiti il percorso scolastico illustrando in un unico contesto, come strumento didattico, la formazione, l'orientamento e i progressi educativi.

La normativa di riferimento (d.lg. 19 aprile 2004, n. 59) prevede a tal fine una documentazione sistematica anche degli elaborati degli alunni, volta a comprendere ed interpretare i loro interessi, le attitudini, i comportamenti e le aspirazioni personali.

Il Portfolio è compilato e aggiornato (nella scuola d'infanzia) dai docenti di sezione, ovvero (nella scuola primaria e secondaria di primo grado) dal docente coordinatore-tutor dell'alunno in collaborazione con altri docenti, alunni e loro genitori, i quali possono apportarvi alcune annotazioni (allegati A, B) e C) del citato decreto).

Il Garante ha ricevuto reclami e segnalazioni di genitori di alunni che lamentano possibili violazioni della riservatezza derivanti dalle modalità con cui istituti scolastici pubblici e privati trattano dati di carattere personale in relazione al Portfolio.

Rispondendo alla richiesta dell'Autorità (nota del 31 maggio 2005), il Ministero dell'istruzione, dell'università e della ricerca-Dipartimento per l'istruzione (lettera del 20 giugno 2005) ha fornito alcune informazioni.

Il Ministero ha anche convenuto sulla necessità di raccogliere nel Portfolio "dati perso-

(*) *G.U.* 8 agosto 2005, n. 183
[doc. *web* n. 1155253]

nali esclusivamente se pertinenti e non eccedenti e, nel caso dei dati sensibili, solamente se indispensabili per la valutazione e l'orientamento dell'alunno"; si è poi dichiarato disponibile ad inviare una nota esplicativa da far pervenire, tramite gli uffici scolastici regionali, a tutte le istituzioni scolastiche, affinché queste si conformino al Codice in materia di protezione dei dati personali nella compilazione e gestione del Portfolio.

A conclusione dell'esame preliminare dei reclami e delle segnalazioni, il Garante ritiene necessario prescrivere a tutti gli istituti scolastici di adottare alcune misure volte a favorire il rispetto dei diritti e delle libertà fondamentali dei cittadini, nonché della loro dignità, con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali (art. 2, comma 1, del Codice), considerata la quantità, la varietà e la delicatezza delle informazioni che possono essere inserite nel Portfolio e l'ingente numero dei minori e familiari interessati.

2. Le principali questioni

Le problematiche rappresentate al Garante riguardano la liceità e la correttezza del trattamento dei dati personali confluenti nel Portfolio, relativi al percorso scolastico e alla vita privata e sociale degli alunni.

Non è previsto, a livello nazionale, un modello tipo di Portfolio sul piano della forma e dei contenuti in dettaglio del documento.

Ciò determina la proliferazione di documenti molto diversi da scuola a scuola, come dimostrano alcuni modelli già esaminati dal Garante, nei quali è richiesto l'inserimento di tipologie di dati personali assai differenti (o è possibile inserirli o chiedere il loro inserimento) e nei quali l'alunno può illustrare rapporti interpersonali di natura privata e vicende familiari.

Dalle risposte fornite ad alcune delle domande proposte nei modelli esaminati (quali, ad esempio, l'indicazione dell'utilizzo della lingua madre solo nel paese di origine, la motivazione alla base di un trasferimento, anche di nazione, del bambino, la descrizione di particolari vicende che hanno caratterizzato il periodo post-natale), possono evincersi informazioni particolarmente delicate come lo stato di adozione di un minore, nei confronti delle quali l'ordinamento impone precise cautele (l. 4 maggio 1983, n. 184, in particolare art. 28).

In alcuni casi, sono richieste informazioni relative al profilo psicologico dell'alunno (descrizione di paure o disagi del minore), al suo stato di salute (notizie su particolari patologie sofferte, eventuali ricoveri ospedalieri), al suo credo religioso, all'ambiente sociale di estrazione (acquisizione di informazioni sui suoi familiari) e ad altri delicati aspetti della sfera privata e a quella di natura strettamente familiare.

La diversità dei modelli di Portfolio agevola, quindi, una più ampia annotazione di informazioni sensibili (che il Codice individua nei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale: art. 4, comma 1, lett. *d*), del Codice).

3. Come trattare i dati personali

La compilazione e la tenuta del Portfolio determina un trattamento di dati personali. L'istituto scolastico frequentato dall'alunno ne è il titolare, stante l'autonomia funzionale, didattica, organizzativa e di ricerca, sperimentazione e sviluppo ad esso riconosciuta (artt. 4, comma 1, lett. *f*) e 28 del Codice; d.P.R. 8 marzo 1999, n. 275).

Tale trattamento deve rispettare le disposizioni del Codice e, in particolare, i principi di seguito richiamati. In caso di loro violazione, i dati personali trattati non possono essere utilizzati (art. 11, comma 2, del Codice).

Principio di finalità (art. 11, comma 1, lett. *b*), del Codice)

47

Il trattamento di dati personali effettuato mediante il Portfolio è consentito solo per raggiungere le finalità individuate direttamente dalla predetta legislazione di riforma (d.lg. n. 59/2004 cit.), ovvero per valutare l'apprendimento e il comportamento degli studenti e per certificare le competenze da essi acquisite.

Non sono perseguibili ulteriori finalità attinenti, ad esempio, all'individuazione del profilo psicologico degli alunni o alla raccolta di informazioni sul loro ambiente sociale e culturale di provenienza.

Principio di necessità (art. 3 del Codice)
Laddove le finalità del Portfolio possono essere perseguite anche senza trattare dati personali, oppure dati identificativi, il trattamento deve riguardare solo dati anonimi (che non riguardano, cioè, interessati identificati o identificabili), oppure, rispettivamente, dati non identificativi (che permettono, cioè, di identificare direttamente un interessato).

Principio di proporzionalità (art. 11, comma 1, lett. *d*), del Codice)
Quando, osservando il principio di necessità, si devono trattare dati personali, deve verificarsi in ogni singola fase del loro trattamento se, e come, determinate operazioni (di raccolta, esame, annotazione, eventuale registrazione, ecc.) siano effettivamente pertinenti e non eccedenti rispetto alla finalità di valutazione dell'alunno.

Principio di indispensabilità (art. 22, comma 3; aut. gen. nn. 2/2004 e 3/ 2004)
Particolare rigore deve essere osservato per quanto riguarda l'eventuale raccolta e registrazione di dati sensibili, i quali sono acquisibili, attraverso una valutazione obiettiva e selettiva, solo se realmente indispensabili per valutare il processo formativo.

4. Prescrizioni da osservare
Con il presente provvedimento, a garanzia degli interessati, il Garante prescrive ai titolari del trattamento di osservare, in attuazione dei predetti principi, anche le seguenti misure volte a conformare pienamente i trattamenti alle vigenti disposizioni in materia di protezione dei dati personali (art. 154, comma 1, lett. *c*), del Codice), invitando il Ministero dell'istruzione, dell'università e della ricerca a recepire le prescrizioni medesime nella nota esplicativa che lo stesso si è riservato di far pervenire, tramite gli uffici scolastici regionali, a tutti gli istituti scolastici.

Ciascun istituto scolastico, in qualità di titolare del trattamento, deve attuare le seguenti misure:

Predisposizione del modello di Portfolio
Nel predisporre il modello di Portfolio, occorre adottare ogni opportuna soluzione per prevenire che vengano raccolti dati sensibili o che sono oggetto, nell'ordinamento, di particolari cautele (*es.*, dati relativi allo stato di affidamento o di adozione), quando gli stessi non siano strettamente indispensabili per raggiungere le finalità di documentazione perseguite. Ciò, con particolare riferimento ai campi nei quali l'alunno potrebbe descrivere alcuni suoi rapporti interpersonali di natura privata o vicende familiari. I riferimenti a tali vicende sono del tutto eventuali nel Portfolio, che deve rimanere uno strumento didattico per favorire solo la personalizzazione dei processi formativi scolastici.

Informare gli interessati
Prima di consentire la compilazione del Portfolio, chi esercita la potestà sull'alunno deve essere informato specificamente in merito al trattamento dei dati personali.

Nell'informativa occorre indicare gli elementi previsti dall'art. 13 del Codice e, in particolare, quali sono le finalità perseguite, se è necessario o facoltativo conferire i dati di natura personale, quali sono le conseguenze di un eventuale rifiuto a fornirli, quali soggetti possono consultare il Portfolio e per quali scopi.

Istruzioni per la compilazione
L'istituto deve impartire idonee istruzioni ai docenti che sovraintendono alla compilazione del Portfolio, affinché adottino particolari cautele nel momento in cui inseriscono o

consentono di inserire dati personali, in particolare quelli particolarmente delicati o sensibili sopra evidenziati.

Presupposti per inserire dati sensibili
Per quanto riguarda i dati sensibili, alcuni presupposti giuridici per trattare i dati sono diversi a seconda che l'istituto scolastico sia di natura privata o pubblica.

Le istituzioni scolastiche private devono acquisire il consenso specifico, preventivo e scritto da parte degli esercenti la potestà; devono poi rispettare le prescrizioni contenute nelle autorizzazioni generali del Garante al trattamento dei dati sensibili (art. 26 del Codice e autorizzazioni nn. 2[1] e 3[2] del 2004, rinvenibili anche sul sito *www.garanteprivacy.it*, efficaci sino al 31 dicembre 2005).

Le istituzioni scolastiche pubbliche non devono richiedere il consenso; devono invece indicare nell'atto di natura regolamentare che deve essere adottato entro il 31 dicembre 2005, in conformità al parere del Garante, i tipi di dati trattabili e le operazioni eseguibili in relazione alla tematica in esame (artt. 20 e 154 del Codice, *cfr. Provv.* Garante del 30 giugno 2005[3]). Mancando un potere regolamentare in capo ai singoli istituti scolastici, e in relazione ai compiti attribuiti al Ministero (art. 75 l. 30 luglio 1999, n. 300), l'Autorità ha rivolto a quest'ultimo l'invito ad adottare uno schema di regolamento per il trattamento dei dati sensibili effettuato da parte di tutti gli istituti scolastici pubblici, da sottoporre al parere del Garante.

Designare gli incaricati
L'istituto deve designare i soggetti che possono accedere ai dati contenuti nel Portfolio quali incaricati o, eventualmente, responsabili del trattamento (artt. 30 e 29 del Codice).

Sicurezza dei dati
Occorre garantire che il trattamento dei dati in questione avvenga nel pieno rispetto delle misure di sicurezza prescritte direttamente dal Codice (artt. 31-36 e Allegato B)).

Garantire l'esercizio dei diritti
Va garantito l'esercizio da parte di tutti gli interessati (e in particolare degli esercenti la potestà), dei diritti individuati dal Codice (art. 7) e, in particolare, del diritto di chiedere l'aggiornamento, la rettificazione, l'integrazione dei dati (quando vi sia interesse), la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione alle finalità di valutazione della formazione scolastica.

Breve conservazione dei dati
Occorre individuare brevi periodi di eventuale conservazione dei dati personali raccolti nel Portfolio, in modo tale che gli stessi siano conservati solo in una forma che consenta di identificare gli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. *e*), del Codice).

Rilascio all'interessato
Il Portfolio (alla stregua di quanto indicato negli allegati B) e C) al citato d.lg. n. 59/2004, secondo cui, nel passaggio al ciclo scolastico successivo, il Portfolio "si innesta su quello portato" dall'alunno) deve essere rilasciato allo studente alla fine del corso degli studi, affinché lo stesso lo consegni, solo ove ciò sia previsto, al nuovo istituto scolastico.

TUTTO CIÓ PREMESSO, IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive agli istituti scolastici di adottare le misure necessarie ed opportune indicate in motivazione, al fine di conformare i trattamenti di dati alle vigenti disposizioni;
b) dispone che copia del presente provvedimento sia inviata al Ministero dell'istruzione dell'università e della ricerca-Dipartimento per l'istruzione, anche per il seguito indicato in motivazione;

(1) [doc. *web* n. 1037043] vers. EN n. 1115285]

(2) [doc. *web* n. 1037047] vers. EN n. 1113111]

(3) [doc. *web* n. 1144445]

47

c) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* ai sensi dell'art. 143, comma 2, del Codice.

Roma, 26 luglio 2005

Il Presidente
Pizzetti

Il Relatore
Paissan

Il Segretario generale
Buttarelli