Contratto di assicurazione sanitaria integrativa del dipendente e protezione dei dati riferiti al coniuge separato

segnalazione relativa al contratto di assicurazione di assistenza sanitaria integrativa stipulato da un datore di lavoro a favore dei propri dirigenti ed estensibile a soggetti appartenenti al nucleo familiare, in qualità di altri beneficiari. Nel caso di specie, il coniuge legalmente separato, sebbene ammesso a fruire delle prestazioni del fondo di assistenza, era tenuto ad inoltrare la propria documentazione sanitaria per il rimborso alla compagnia di assicurazione per il tramite del coniuge assicurato: tale circostanza ha indotto il segnalante, a tutela della propria riservatezza, a chiedere al fondo di poter gestire direttamente ed autonomamente le proprie pratiche.

Il fondo, che in un primo momento aveva negato siffatta possibilità, ostandovi il regolamento di assistenza (approvato tramite accordo collettivo sottoscritto dalle associazioni sindacali), a seguito della richiesta di informazioni da parte dell'Ufficio del Garante volta a chiarire le eventuali ragioni ostative che avrebbero impedito al segnalante, ove legittimato a godere delle prestazioni assicurative, ad inviare direttamente la pertinente documentazione sanitaria all'assicurazione, considerata la delicatezza del caso, si è dichiarato disposto a "derogare" al predetto regolamento (consentendo al segnalante la gestione diretta delle relative pratiche ed impegnandosi a tener in conto di siffatte problematiche connesse con l'esigenza di riservatezza e di protezione dei dati sensibili degli altri beneficiari della polizza, nell'ambito dei negoziati sindacali per la redazione di un nuovo regolamento).

Al di là di questo caso specifico, sono comunque all'esame dell'Autorità le modalità con le quali, nel settore assicurativo, vengono gestiti analoghi contratti, con particolare riferimento alla presenza di possibili modalità individualizzate di trasmissione dei dati (non di rado sanitari) relativi a familiari, potendosi presentare situazioni delicate connesse alla conoscibilità delle informazioni relative alla salute dei congiunti (e destinate ad acuirsi in presenza di particolari circostanze, quali il caso del coniuge separato o di figli, pur maggiorenni, a carico dell'assicurato).

Dati assicurativi e principio di qualità

Altro caso degno di menzione riguarda alcune segnalazioni aventi ad oggetto la ricezione di avvisi di scadenza di polizze assicurative (note di studi legali o di società di recupero crediti), volti a sollecitare pagamenti. Rispetto a tali polizze, per le quali risultava essere stato già esercitato il diritto di recesso da parte degli assicurati (artt. 172 e 177 d.lg. 7 settembre 2005, n. 209) le ulteriori operazioni di trattamento (nella forma della richiesta del pagamento) lasciavano presupporre un mancato aggiornamento dei dati personali relativi agli assicurati.

A seguito dei riscontri forniti e delle successive osservazioni ed integrazioni documentali pervenute dai segnalanti, rispetto ad un caso il procedimento è stato definito senza l'adozione di provvedimenti da parte dell'Autorità, risultando il mancato aggiornamento dei dati imputabile alla pendenza di controversie aventi ad oggetto la regolarità e la tempestività dell'esercizio del diritto di recesso. Nei confronti di un altro gruppo assicurativo, con esclusivo riferimento al trattamento posto in essere da una singola agenzia, è tuttora in corso l'attività istruttoria, attesa la discordanza degli elementi che emergeva dalla documentazione in atti.

9.3. Marketing

Regole per la raccolta del consenso per finalità di *marketing*

Nel 2005 sono state affrontate differenti questioni inerenti al trattamento di dati per finalità di *marketing*, alcune delle quali hanno già formato oggetto di interventi in passato, riferite al trattamento di dati per svolgere attività pubblicitarie e di vendita diretta o per il compimento di ricerche di mercato.

Numerosi, in proposito, sono stati i ricorsi, le segnalazioni e i reclami relativi alla ricezione di lettere, telefonate, fax ed altre comunicazioni, spesso effettuate mediante posta elettronica, relative ad informazioni pubblicitarie non richieste dagli interessati. Si è inoltre esaminato approfonditamente il profilo dei trattamenti di dati personali in occasione di operazioni a premio e, più in generale, in relazione a fenomeni di "fidelizzazione" della clientela (*cfr. Relazione* 2004, p. 70). Hanno formato, altresì, oggetto di trattazione numerose segnalazioni tanto con riguardo ai profili inerenti alle informazioni da rendere agli interessati, quanto in relazione alle modalità di acquisizione del loro consenso –talvolta mediante l'utilizzo di moduli resi disponibili *on-line*– in occasione del compimento di attività di raccolta di dati per il perseguimento della finalità in esame. Se, con riguardo alle informazioni da rendere, si riscontra non di rado che esse sono difettose o comunque non sufficientemente chiare, in relazione al consenso gli operatori economici sembrano prediligere formulazioni generali, tese a ricomprendere più finalità, tra loro diverse e talvolta incompatibili.

Nel 2005, è stata rivolta attenzione anche alle numerose istanze e segnalazioni pervenute in ordine alle modalità prescelte dagli operatori del settore al fine di acquisire, in occasione dell'instaurazione di un rapporto contrattuale, il consenso degli interessati al trattamento dei dati che li riguardano per perseguire finalità di *marketing*.

A questo proposito, con un *provvedimento* del 12 ottobre 2005 [doc. *web* n. 1179604], si è affermato che è non "libero", ma "necessitato" (e, quindi, invalido), il consenso al trattamento dei dati per finalità promozionali reso senza una libera scelta aderendo ad un testo predisposto unilateralmente dalla controparte contrattuale quale condizione per il conseguimento della prestazione principale richiesta. In tal modo, i dati personali raccolti lecitamente dal titolare (e conferiti dall'interessato) per perseguire una finalità determinata (dare esecuzione al rapporto contrattuale, finalità che non richiede il consenso), vengono di fatto piegati ad un utilizzo diverso dallo scopo originario che ne giustifica la raccolta, in violazione del principio di finalità (art. 11, comma 1, lett. *b*), del Codice).

Alla luce di tali considerazioni, pur consentendo che si potesse continuare a perseguire le finalità principali del contratto connesse alla prenotazione, all'acquisto e al recapito di biglietti (art. 24, comma 1, lett. *b*), del Codice), il Garante ha quindi prescritto di adottare alcune necessarie modifiche al modello per la manifestazione del consenso al trattamento dei dati, affinché quest'ultimo risultasse "modulare", ossia prestato dagli interessati distintamente per ciascuna distinta finalità perseguita.

Il consenso *on-line*

L'attività sul tema dell'Autorità ha riguardato anche le modalità di raccolta *on-line* del consenso della clientela. A questo proposito, si è colta l'occasione per ribadire quanto già affermato anche in passato in merito alla necessità che i sistemi informativi dei siti *web* vengano configurati in modo da consentire agli interessati di esplicare pienamente il proprio diritto all'autodeterminazione informativa, prevedendo opzioni di tipo "positivo" (mediante l'inserimento di caselle di scelta, anziché di campi pre-selezionati su una tra le possibili scelte), così da permettere ad essi di esprimere liberamente le proprie scelte in ordine alle finalità legittimamente perseguibili da parte del titolare del trattamento (*cfr.* il già citato *Provv.* 12 ottobre 2005 [doc. *web* n. 1179604]).

In un caso particolare, anche alla luce di quanto sopra rappresentato, è stata ad esempio constatata la non conformità alle norme in materia di protezione dei dati della scelta di raccogliere in un unico contesto (si trattava delle condizioni generali di contratto), sia il "consenso" del cliente per accedere *on-line* ad alcuni servizi, sia il consenso per trattare i dati conferiti per la fruizione di quest'ultimi allo scopo di perse-

guire una finalità diversa, quale quella dell'invio di comunicazioni commerciali in forma elettronica intese a promuovere iniziative proprie o a veicolare iniziative promozionali nell'interesse di terzi. Si è nuovamente ritenuto che un consenso manifestato nei termini appena descritti non può ritenersi valido, atteso che i clienti devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso –quando questo è necessario– per ciascuna distinta finalità perseguita dal titolare (*Provv.* 3 novembre 2005 [doc. *web* n. 1195215]).

Il Garante ha poi precisato che è possibile basare su un altro presupposto tale trattamento di dati qualora ricorrano le condizioni di cui all'art. 130, comma 4, del Codice, norma in base alla quale il titolare del trattamento che utilizzi le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio ai fini di vendita diretta di propri prodotti o servizi (e sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato), può non richiedere il consenso qualora l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. Affinché in tale ipotesi il trattamento si configuri come legittimo, occorre quindi accordare al cliente la possibilità di opporsi in maniera agevole e gratuitamente all'utilizzo delle coordinate di posta elettronica per finalità di vendita diretta, sin dalla fase di raccolta dei dati ("inizialmente", secondo la prescrizione dell'art. 130, comma 4, del Codice), come pure in occasione dell'invio di ogni comunicazione successiva, possibilità che non veniva accordata all'interessato nel caso esaminato.

Il Garante ha infine evidenziato che la circostanza dell'"assorbimento" del consenso all'utilizzo dei dati per finalità di vendita diretta nelle condizioni generali di contratto (destinate a regolare solo la fornitura dei servizi propriamente intesi), è tra l'altro idonea di per sé a evidenziare una violazione della disposizione richiamata, che intende salvaguardare la facoltà di autodeterminazione dell'interessato, anche nella forma della libera opposizione al trattamento dei dati, in ordine all'utilizzo delle proprie coordinate di posta elettronica al fine di vendita diretta.

Il trattamento dei dati dei minori

Sempre con riguardo al profilo della raccolta del consenso degli interessati, l'Autorità ha affrontato ulteriori aspetti in merito alle operazioni di trattamento di dati personali concernenti minori. In proposito, il Garante ha puntualizzato che la raccolta e le successive operazioni di trattamento sui dati relativi a minori possono essere effettuate lecitamente, una volta resa l'informativa nei termini di cui all'art. 13 del Codice, dopo aver acquisito il consenso espresso dei soggetti titolari della potestà genitoriale (art. 23 del Codice, artt. 316 e ss. c.c.; *v.* anche punto 2.6 del codice di autoregolamentazione Fedma (Federazione europea del *marketing* diretto), rispetto al quale il Gruppo art. 29 si è espresso favorevolmente con parere n. 3/2003 il 13 giugno 2003; *Provv.* 30 novembre 2005 [doc. *web* n. 1212652]).

Operazioni a premio e carte di fidelizzazione

Come anticipato, quello delle carte e dei programmi di "fidelizzazione" della clientela è un fenomeno sempre più diffuso tra la popolazione: interessa in primo luogo il settore della *cd.* grande distribuzione (supermercati), ma anche quello della prestazione di servizi nei trasporti, nel credito, nella telefonia, nell'editoria, nel noleggio, ecc. Preso atto di tale crescente diffusione, conclusi gli accertamenti e la consultazione pubblica avviata sul tema (v. *Relazione* 2004, p. 70), volti ad acquisire gli elementi necessari per verificare la conformità alle norme sulla protezione dei dati personali delle modalità di trattamento di dati personali prescelte dagli operatori di settore, l'Autorità ha fissato alcune prescrizioni per l'uso corretto dei dati dei clienti da parte dei soggetti che rilasciano le *cd.* "carte di fidelizzazione" (*Provv.* 24 febbraio 2005 [doc. *web* n. 1103045]).

Alla luce degli elementi acquisiti il Garante ha constatato che in occasione del rilascio delle carte di fidelizzazione (spesso mediante compilazione di questionari) e della loro successiva utilizzazione (attraverso la registrazione dell'acquisto di beni e servizi) vengono raccolti dati personali dei clienti e, a volte, dei loro familiari (tra i quali, dati anagrafici, titolo di studio, professione, interessi, abitudini di consumo, modalità di acquisto, volumi di spesa effettuata, ecc.), e che tali informazioni sono spesso utilizzate, senza che gli interessati ne abbiano piena conoscenza e possano acconsentire al loro uso, anche per monitorarne in dettaglio i comportamenti o le loro propensioni al consumo; per creare, cioè, "profili" individuali o di gruppo volti a confrontarne le abitudini di consumatori con altri clienti.

Le regole individuate nel provvedimento riguardano pertanto le tre principali finalità per le quali i dati personali degli interessati sono di regola raccolti e trattati: la *cd.* fidelizzazione in senso stretto, che viene realizzata attribuendo vantaggi connessi all'uso della carta (di regola consistenti nella partecipazione ad operazioni a premio), la *cd.* profilazione, volta ad analizzare abitudini e scelte di consumo della clientela, e lo svolgimento di attività di *marketing* diretto.

Il primo obbligo previsto per chi rilascia carte di fedeltà è quello di informare in maniera chiara e completa i clienti sull'uso che verrà fatto dei dati che li riguardano, tenendo conto in maniera differenziata delle diverse finalità perseguite. In base a quanto indicato dall'Autorità, l'informativa al cliente deve essere chiaramente evidenziata all'interno dei moduli di sottoscrizione utilizzati e risultare agevolmente individuabile rispetto alle altre clausole del regolamento. In particolare, deve essere posta in evidenza l'eventuale attività di profilazione e/o quella di *marketing* chiarendo che, per queste ultime due finalità, il conferimento dei dati è libero (e facoltativo rispetto alle ordinarie attività legate alla fidelizzazione in senso stretto) e che il consenso va prestato distintamente per ciascuna di esse.

Il Garante ha poi stabilito che chiunque ponga in essere operazioni a premio (o programmi di fidelizzazione) deve ridurre al minimo l'uso delle informazioni personali e utilizzare solo informazioni pertinenti e non eccedenti (artt. 3 e 11 del Codice). In particolare, per quanto riguarda la fidelizzazione, possono essere trattati senza acquisire il consenso degli interessati solo i dati necessari per attribuire vantaggi connessi all'utilizzo della carta, ovvero i dati correlati all'identificazione dell'intestatario o relativi al volume di spesa globale realizzato, di regola senza riferimento al dettaglio dei singoli prodotti acquistati.

Per l'attività di profilazione, occorre invece il consenso dell'interessato per trattare le informazioni relative agli acquisti effettuati e quelle ulteriori raccolte all'atto dell'adesione del cliente all'iniziativa, ed è necessario adempiere altresì all'obbligo di notificazione (art. 37, comma 1, lett. *d*), del Codice).

Riguardo all'attività di *marketing* possono essere raccolti, sempre con il consenso dell'interessato, i dati necessari all'invio di materiale pubblicitario o di comunicazioni commerciali.

Il Garante ha disposto che. allo stato, la conservazione dei dati personali dei clienti relativi al dettaglio degli acquisti non può superare un anno rispetto alle finalità di profilazione, e due anni per i dati raccolti a fini di *marketing.*

È stato altresì precisato che le carte fedeltà già rilasciate non dovevano essere annullate laddove i dati raccolti venissero utilizzati, sulla base di un'adeguata informativa, ai soli fini di sconti, premi, *bonus,* servizi accessori, facilitazioni di pagamento, sul presupposto che in tali casi non è necessario il consenso degli interessati e che questo resta, invece, necessario quando i dati vengono utilizzati per il perseguimento di altre finalità quali la profilazione e il *marketing* (*Comunicato stampa* 29 luglio 2005).

Per quanto attiene da ultimo all'interconnessione con altre banche dati, va ricordato che il Garante ha adottato un apposito provvedimento in materia di utilizzo a fini di *marketing* e di profilazione degli elenchi "categorici" (*cfr.* par. 15.3), le cui prescrizioni sono ora da coordinare con il disposto dell'art. 19-*bis* l. n. 51/2006 (su cui *v.* par. 1.3).

9.4. *Impresa*

Dati personali e recupero crediti

Ha formato oggetto di esame un numero elevato di segnalazioni relative ai profili di protezione dei dati personali rispetto alle attività di recupero dei crediti. A conclusione dell'istruttoria avviata in tale delicata materia e sulla base dei diversi accertamenti effettuati, il Garante ha constatato l'illecito utilizzo, da parte di diversi operatori, dei dati personali relativi ai debitori.

Si è in particolare riscontrato come, attraverso soggetti incaricati del recupero, venissero poste in essere modalità particolarmente invasive di ricerca, di presa di contatto e di sollecitazione al pagamento delle somme dovute: visite a domicilio o sul posto di lavoro degli interessati, reiterate sollecitazioni al telefono fisso o sul cellulare, utilizzo di sistemi automatizzati di chiamata senza operatore, invio di cartoline o di plichi postali con l'indicazione chiaramente visibile della scritta "recupero crediti" o "preavviso esecuzione notifica" o diciture analoghe, affissione di avvisi di mora sulla porta di casa. Spesso, i dati personali relativi ai componenti di intere famiglie risultavano inoltre inseriti nelle banche dati del soggetto creditore o delle società di recupero crediti.

Il Garante ha conseguentemente adottato un provvedimento a carattere generale con il quale ha prescritto alle società di recupero crediti e a quanti –finanziarie, banche, concessionari di pubblici servizi, compagnie telefoniche– svolgono tale attività direttamente, le misure alle quali attenersi per non incorrere in illeciti e per rispettare i principi posti a tutela dei diritti della persona: fermo restando il diritto del creditore a tutelare le proprie ragioni, il suo esercizio non deve infatti tradursi in abuso, dovendo essere improntato ai generali principi di buona fede e di correttezza contemplati nel nostro ordinamento.

Sono state pertanto considerate illecite tutte le modalità di recupero del credito le quali, ancorché finalizzate all'esercizio di diritti, risultino lesive della sfera personale dei debitori e della loro dignità (*Provv.* 30 novembre 2005 [doc. *web* n. 1213644]).

Non è risultato lecito, in particolare, comunicare ingiustificatamente informazioni relative ai mancati pagamenti a soggetti diversi dall'interessato (*ad es.*, familiari, colleghi di lavoro o vicini di casa) ed esercitare indebite pressioni su quest'ultimo al fine di sollecitare il pagamento di somme dovute. Non è risultato consentito, altresì, ricorrere a telefonate pre-registrate, anche perché attraverso questa modalità persone diverse dal debitore, in assenza di adeguate garanzie, potrebbero venire a conoscenza della sua eventuale inadempienza.

È emersa anche l'illiceità dell'affissione da parte degli incaricati del recupero crediti di avvisi di mora su porte di abitazioni, trattandosi di modalità che rende possibile la diffusione dei dati personali dell'interessato ad una serie indeterminata di soggetti. Non deve inoltre rendersi visibile a persone estranee il contenuto di una comunicazione, come può avvenire ad esempio mediante l'utilizzo di cartoline postali o con l'invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili. È necessario, invece, che le sollecitazioni di pagamento vengano portate a conoscenza del solo debitore, usando plichi chiusi e senza scritte specifiche.

Gli incaricati delle società non possono poi usare altri dati se non quelli necessari all'esecuzione del mandato (dati anagrafici, codice fiscale, ammontare del credito, recapiti telefonici).

Salvo l'assolvimento di specifici obblighi di legge che può richiedere una conservazione prolungata dei dati raccolti (*ad es.*, per rendere conto delle attività svolte), una volta portato a termine l'incarico i dati non possono formare oggetto di ulteriore trattamento. La loro eventuale conservazione ulteriore deve essere realizzata con modalità tali, comunque, da precluderne agli incaricati del trattamento l'ordinaria consultabilità (adottando opportune misure logiche o provvedendo alla trasposizione dei dati in archivi separati).

Dati personali e servizi radiotaxi

Muovendo da alcune segnalazioni di singoli e di associazioni per la tutela dei diritti dei consumatori, l'Autorità ha valutato la liceità o meno dei trattamenti di dati personali della clientela effettuati da soggetti che forniscono servizi radiotaxi.

Gli accertamenti hanno permesso di constatare che questi ultimi raccolgono, generalmente per via telefonica, richieste di corse taxi nell'interesse dei titolari di licenza (art. 7 l. n. 21/1992). Di regola, le informazioni raccolte si esauriscono nel solo indirizzo di prelievo; in altri casi, invece, formano oggetto di trattamento anche il numero di telefono e il nominativo del cliente (eventualmente associando, in modo automatizzato, il numero telefonico a dati ricavati da elenchi pubblici). In casi limitati, vengono registrate informazioni aggiuntive concernenti comportamenti tenuti dal cliente a seguito della chiamata (*ad es.*, assenza presso l'indirizzo di prelievo o mancato pagamento della corsa).

Con un *provvedimento* del 26 luglio 2005 [doc. *web* n. 1151997], il Garante ha affermato che è lecito utilizzare solo i dati necessari per mettere in contatto il cliente con il taxi indicato per effettuare la corsa, o comunque utili per dare attuazione al relativo rapporto contrattuale (quali l'indirizzo di prelievo, il nominativo, l'eventuale numero telefonico fisso o mobile), agevolando in tal modo l'esatta esecuzione della prestazione (*ad es.*, per segnalare una sostituzione del taxi o per assicurarsi che il servizio venga reso alla persona che lo ha effettivamente richiesto). L'Autorità ha aggiunto che, in base a quanto previsto dall'art. 11, comma 1, lett. *b*), del Codice, non possono essere registrati dati sui percorsi effettuati dai clienti o relativi ad eventuali inadempimenti loro attribuiti, fatta salva l'esigenza di far valere o difendere un diritto in sede giudiziaria; né possono essere conservate informazioni relative all'assenza dei clienti presso l'indirizzo di prelievo indicato oltre il tempo strettamente necessario a rispondere ad eventuali contestazioni, considerato che il loro trattamento ha una finalità del tutto diversa da quella perseguita nel rendere possibile il trasporto della clientela (unica finalità per la quale il gestore del servizio radiotaxi può raccogliere lecitamente i dati).

Al di fuori delle operazioni di raccolta e di successivo trattamento dei dati della clientela preordinati alla ordinaria prestazione del servizio (in relazione alla quale trova applicazione l'art. 24, comma 1, lett. *b*), del Codice), il trattamento delle informazioni relative ai clienti per perseguire scopi ulteriori (*ad es.*, a fini di *marketing* o per compiere ricerche di mercato, o ancora al fine di fornire, anche su registrazione o abbonamento, servizi aggiuntivi rispetto alla singola corsa di volta in volta richiesta) richiede infatti il consenso specifico degli stessi.

È stato altresì precisato che, una volta espletato il servizio, i dati non più necessari devono essere cancellati o trasformati in forma anonima, salva l'osservanza di eventuali e puntuali obblighi di legge che ne legittimino l'ulteriore conservazione; i dati relativi alla clientela possono essere conservati solo per scopi compatibili con il servizio reso (restituzione oggetti smarriti, contestazioni sulla corsa), per un tempo massimo di trenta giorni.

Con riguardo agli ulteriori obblighi previsti dalla normativa contenuta nel Codice, il Garante ha prescritto ai gestori di servizi radiotaxi di informare i propri clienti al momento del contatto (di regola telefonico) circa l'uso che verrà fatto dei dati che li riguardano, con particolare riferimento alle differenti finalità perseguite e alla tipologia dei dati personali utilizzati per ciascuna di esse. Tale informativa può essere resa, previa motivata e specifica richiesta rivolta all'Autorità, in forma semplificata, al telefono –in sede di prenotazione del servizio– e deve essere integrata mediante l'affissione all'interno del taxi di un testo contenente gli elementi menzionati nell'art. 13 del Codice. Al riguardo, l'Autorità ha predisposto un modello di informativa di riferimento per i gestori di servizi radiotaxi cui uniformarsi, allegandolo, a tal fine, al provvedimento sopra citato.

Dati personali e catene alberghiere

A seguito di accertamenti disposti nei confronti di una nota catena alberghiera, l'Autorità si è pronunciata in ordine ai trattamenti di dati raccolti nell'ambito dell'esecuzione della prestazione alberghiera (*Provv.* 9 marzo 2006 [doc. *web* n. 1252220]). Il Garante ha rilevato che, nel modello di informativa reso alla clientela, anche in sede di prenotazione, devono essere in particolare evidenziate le caratteristiche delle attività di profilazione e di promozione commerciale eventualmente svolte. Gli interessati devono essere posti in condizione di esprimere un consenso differenziato, debitamente informato, rispetto a quello manifestato con l'adesione al programma di fidelizzazione. In particolare, nello svolgimento delle operazioni (anche per via telematica) per il rilascio di una carta di fidelizzazione, la società deve specificare la finalità di *marketing* perseguita, precisando nell'informativa che il consenso e, dunque, il conferimento dei dati a tale scopo, è facoltativo ed indipendente rispetto alla finalità di fidelizzazione in senso stretto (art. 23 del Codice).

Il consenso dell'ospite al trattamento dei dati personali a sé riferiti non è in termini generali necessario, sia nella parte in cui si deve adempiere a specifiche disposizioni di legge (ad esempio, per le menzionate finalità di pubblica sicurezza), sia per ciò che attiene all'ordinario servizio di albergo, quando il trattamento dei relativi dati è indispensabile per eseguire obblighi derivanti dal contratto o per adempiere, anche in fase precontrattuale, a specifiche richieste dell'ospite-interessato, ad esempio a seguito dell'adesione ad una operazione a premi (art. 24, comma 1, lett. *a*) e *b*), del Codice).

Ogni altra finalità del trattamento che comporti un'ulteriore conservazione dei dati personali raccolti (*ad es.*, come avvenuto nel caso esaminato, ricerche di mercato, operazioni di *marketing* o profilazioni) necessita, invece, del consenso specifico e informato, espresso distintamente da parte del cliente (art. 23 del Codice). Tale autodeterminazione non è assicurata quando si raccoglie il consenso in modo indifferenziato per perseguire finalità in realtà distinte tra loro, quali la definizione dei profili della clientela e l'invio alla stessa di comunicazioni commerciali (*marketing*), ben potendo essere ciascuna di esse perseguita singolarmente in presenza di autonome valutazioni e determinazioni dell'interessato.

Il Garante è intervenuto anche in ordine al profilo della durata massima di conservazione dei dati raccolti, atteso che nel medesimo caso non era stato stabilito un termine di conservazione dei dati presenti nella banca dati della clientela, accessibili nella loro interezza solo dalle funzioni centrali della società e, limitatamente agli ultimi tre soggiorni di ciascun cliente, anche da parte delle singole strutture alberghiere. In applicazione dei principi di pertinenza e proporzionalità, si è prescritto quindi di identificare i tempi massimi di conservazione dei dati trattati alla luce delle finalità in concreto perseguite dalla società, nonché delle scelte dell'interessato in ordine al trattamento medesimo. In particolare, nell'ipotesi in cui il trattamento dei dati sia preordinato alla realizzazione delle operazioni a premio, la

conservazione non deve protrarsi oltre la scadenza del termine della stessa indicato nel regolamento (o della sua eventuale proroga); con specifico riguardo all'attività di profilazione della clientela il Garante ha poi ribadito il termine massimo di dodici mesi decorrenti dalla registrazione delle informazioni, conformemente a quanto stabilito nel *provvedimento* del 24 febbraio 2005 [doc. *web* n. 1103045].

Per quanto attiene quindi alle finalità di *marketing* e di vendita diretta, si è precisato che resta impregiudicata la facoltà degli interessati di opporsi al trattamento dei dati personali che li riguardano (art. 7, comma 4, lett. *b*), del Codice; *v.* anche, per quanto riguarda le "coordinate di posta elettronica", l'art. 130, comma 4, del Codice).

Da ultimo, nel dichiarare illecito il trattamento dei dati personali della clientela effettuato dalla catena alberghiera in ordine ai profili dell'omessa e incompleta informativa, della mancata acquisizione del consenso per le attività connesse alla definizione dei profili individuali in relazione a scelte e preferenze di consumo e per svolgere operazioni di *marketing* nell'ambito della gestione dell'operazione a premi, nonché dell'omessa notificazione dei trattamenti volti a definire il profilo degli interessati e ad analizzarne abitudini o scelte di consumo, il Garante ha in conclusione vietato, ai sensi dell'art. 154, comma 1, lett. *d*), del Codice, la prosecuzione delle operazioni di trattamento di dati personali effettuate in violazione di legge.

Modalità di voto e delibere assembleari delle società cooperative

Con nota del 10 gennaio 2005, l'Ufficio del Garante si è soffermato sull'utilizzabilità, nell'ambito delle società cooperative a r.l., della modalità di voto a scrutinio segreto ai fini dell'adozione delle relative delibere assembleari.

Muovendo dal rinvio alle disposizioni sulle società per azioni contenuto nell'art. 2519 c.c. in tema di norme applicabili alle società cooperative, è stato rilevato che l'art. 2375 c.c., nella formulazione derivante dalla recente riforma (d.lg. 17 gennaio 2003, n. 6), prevede, in termini generali, la necessità di indicare nel verbale assembleare delle società per azioni modalità e risultati delle votazioni, e di consentire, anche per allegato, l'identificazione dei soci favorevoli, astenuti o dissenzienti. È stato altresì evidenziato l'applicabilità, alle modalità di votazione, dell'art. 2368 c.c., nella parte in cui ammette che l'atto costitutivo possa stabilire norme particolari per la "nomina delle cariche sociali".

Alla luce di tali considerazioni, con riferimento al caso di specie (rispetto al quale la società aveva adottato il sistema di voto a scrutinio palese nelle proprie deliberazioni attraverso l'approvazione di un'autonoma clausola statutaria), l'Autorità si è espressa nel senso che la propria competenza relativa alla liceità e correttezza del trattamento dei dati in relazione al Codice non consente un intervento inibitorio o interdittivo in materia, non disponendo del potere di vincolare l'autonomia contrattuale dei soci di una società a r.l. per introdurre, in deroga al predetto principio civilistico dello scrutinio palese, una clausola statutaria (peraltro controversa in giurisprudenza) che preveda lo scrutinio segreto.

Giochi olimpici invernali

Nel 2005 l'Autorità ha avviato incontri tecnici volti ad esaminare alcune questioni sottoposte all'attenzione dell'Ufficio del Garante dai rappresentanti del Comitato organizzatore dei XX Giochi olimpici invernali, in programma a Torino nel 2006. L'intento perseguito attraverso tale collaborazione è stato quello di garantire, nel corso dello svolgimento di tale manifestazione, il rispetto della riservatezza dei dati concernenti i vari soggetti coinvolti (quali visitatori, dipendenti e atleti), considerata anche l'importanza e la portata dell'evento.

In occasione di tali incontri sono stati affrontati, anche alla luce dei provvedimenti già adottati dal Garante, e in aggiunta ad alcuni profili relativi ai principi generali in materia di trattamento dei dati (quali l'obbligo di rendere l'informativa agli interessati, di notificare i trattamenti al Garante ai sensi dell'art. 37 del Codice e di

designare incaricati ed eventuali responsabili del trattamento), altri più specifici aspetti concernenti l'utilizzazione di sistemi di videosorveglianza, l'attivazione di *call center*, l'adozione di adeguate misure di sicurezza dei dati e le modalità di contatto con la clientela. Inoltre, hanno formato oggetto di esame i nuovi modelli predisposti dal Comitato per informare la clientela, presso i relativi punti vendita, ma anche *on-line* e attraverso il *call center*, all'atto dell'acquisto e/o della prenotazione dei biglietti, nonché per richiedere il suo specifico consenso all'eventuale uso dei dati che la riguardano per compiere operazioni di *marketing*.

9.5. *Trasferimento dei dati personali all'estero*

Autorizzazioni del Garante al trasferimento di dati verso Paesi terzi

Come riportato nella *Relazione* 2004, il Codice (Parte I, Titolo VII) ha disciplinato il trasferimento dei dati all'estero completando il recepimento della direttiva comunitaria 95/46/Ce e ribadendo il principio generale in base al quale il flusso di dati verso un Paese esterno all'Unione europea è autorizzato soltanto quando sussiste il consenso dell'interessato o sulla base di almeno uno degli altri presupposti di liceità (art. 43 del Codice), o se il Paese di destinazione assicura un livello adeguato di protezione.

In quest'ambito l'attività del Garante ha assunto particolare rilievo nel corso del 2005 in corrispondenza all'adozione di alcune decisioni comunitarie concernenti il livello di adeguatezza di protezione di dati personali garantito da Paesi extra-Ue. Il 9 giugno 2005 il Garante ha autorizzato, con due deliberazioni (pubblicate in *G.U.* 25 luglio 2005, n. 171) i trasferimenti dei dati personali dal territorio italiano verso l'Argentina e l'Isola di Man, considerato che, stando alla valutazione svolta dalla Commissione europea nelle decisioni assunte il 30 giugno 2003 (n. 2003/490/Ce) e il 28 aprile 2004 (n. 2004/411/Ce), deve ritenersi che tali Paesi garantiscano nel proprio ordinamento un livello adeguato di protezione dei dati personali (*Autorizzazioni* 9 giugno 2005 [doc. *web* n. 1151846 e n. 1151889]).

Va segnalata, inoltre, la pubblicazione (in *G.U.* 22 luglio 2005, n. 169) della precedente deliberazione n. 6 del 7 settembre 2004 [doc. *web* n. 1139333], con cui il Garante aveva ritenuto parimenti adeguato il livello di protezione dei dati personali nel Baliato di Guernsey, come evidenziato nella decisione della Commissione europea del 21 novembre 2003 n. 2003/821/Ce (*v. Relazione* 2004, pag. 73).

Il Garante ha reso quindi pienamente operative nell'ordinamento interno le tre predette decisioni della Commissione europea che vanno ad affiancarsi alle altre pronunzie in materia, concernenti il livello di adeguatezza di Canada, Svizzera e Ungheria (anteriormentemente al suo ingresso nell'Ue), e rispetto alle quali il Garante ha simmetricamente rilasciato negli anni precedenti apposite autorizzazioni.

L'Autorità, come previsto dai compiti attribuiti dal Codice, si è riservata di svolgere controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti stessi e di adottare, qualora si riveli necessario, eventuali provvedimenti di blocco o di divieto.

Le clausole contrattuali per il trasferimento

Nel corso del 2005 sono state sottoposte all'attenzione dell'Ufficio del Garante alcune iniziative intraprese in relazione alla circolazione di dati personali da parte di una società avente sede negli Stati Uniti, facente parte di un gruppo societario operante a livello internazionale, volte a garantire il rispetto della normativa comunitaria e nazionale nell'ambito delle operazioni di trasferimento di dati personali *infra*-gruppo concernenti differenti tipologie di interessati (quali clienti, dipendenti e fornitori delle società del gruppo).

Al fine di rendere lecite le operazioni sopra menzionate la società interessata ha sottoscritto con altre società controllate e collegate, aventi sede in vari Stati dell'Ue ed in alcuni Paesi terzi, un contratto *cd.* globale volto a regolamentare i flussi transfrontalieri di dati personali all'interno del gruppo.

Sulla base di alcune prime osservazioni formulate dall'Ufficio e da altre autorità di controllo europee interpellate, nell'ambito del rapporto di collaborazione instauratosi, è stato predisposto un nuovo schema di "contratto integrativo" volto a regolamentare specificamente i flussi di dati oggetto di trattamento nel gruppo, dalle società europee alla società americana e alle altre affiliate stabilite al di fuori dell'Ue. Tale schema di contratto, denominato *Eu Addendum*, basato sostanzialmente sulle clausole contrattuali-tipo per trasferire dati a responsabili del trattamento stabiliti in Paesi terzi (di cui all'allegato della decisione del 27 dicembre 2001 della Commissione europea n. 2002/16/Ce, e relativa *autorizzazione* del Garante del 10 aprile 2002 [doc. *web* n. 1065361]), è in corso di valutazione.

Il modello alternativo di clausole contrattuali tipo

Un modello alternativo di clausole contrattuali-tipo (definito "Insieme II"), rispetto a quelle già approvate con la decisione della Commissione europea n. 2001/497/Ce (del 15 giugno 2001), ha formato oggetto della decisione della Commissione del 27 dicembre 2004, n. 2004/915/Ce (pubblicata in *G.U.C.E.* 29 dicembre 2004 L 385/74) che ha in parte modificato la prima decisione ed introdotto l'insieme alternativo predetto di clausole contrattuali-tipo. Tali clausole, secondo la Commissione, costituiscono anch'esse garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi in caso di trasferimento di dati personali verso Paesi terzi a norma della direttiva 95/46/Ce.

Le clausole, elaborate dalla Camera di commercio internazionale (Icc) e da altre organizzazioni commerciali, hanno formato oggetto di un primo parere del Gruppo art. 29 (parere 8/2003, 17 dicembre 2003) il quale aveva suggerito alcune modifiche per rendere il livello di tutela equiparabile a quello delle clausole già approvate dalla Commissione il 15 giugno 2001 e rese operative in Italia con l'*autorizzazione* del Garante del 10 ottobre 2001 [doc. *web* n. 42156].

Le clausole trovano applicazione in caso di trasferimenti di dati effettuati a partire dal territorio dello Stato, da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un diverso titolare del trattamento (soggetto importatore), residente in un Paese terzo che non assicura un livello di protezione adeguato, e possono essere utilizzate alternativamente rispetto alle clausole contrattuali *standard* individuate con la decisione del 2001 (ora definite "Insieme I"). Il Garante ha reso operative tali clausole nell'ordinamento interno con un'*autorizzazione* del 9 giugno 2005 [doc. *web* n. 1151949].

Utilizzo delle *cd.* *binding corporate rules*

Con particolare riferimento ai trasferimenti di dati fra società appartenenti ad uno stesso gruppo multinazionale, il Gruppo art. 29 ha evidenziato l'opportunità di introdurre nell'ambito di tali gruppi, in aggiunta alle clausole-tipo già predisposte, ulteriori garanzie per la protezione dei dati personali, ossia regole di comportamento che avrebbero natura vincolante per tutti i soggetti che ne fanno parte (*Binding Corporate Rules for International Data Transfers*).

Il 14 aprile 2005 il Gruppo ha approvato due documenti (WP 107 e WP 108; *cfr. Newsletter* del 25 aprile-1° maggio 2005), individuando le procedure di verifica attraverso le quali le imprese multinazionali potrebbero vedere riconosciuta in tutti i Paesi dell'Ue la validità delle *cd.* "regole vincolanti nell'impresa" ai fini del trasferimento di dati personali verso Paesi terzi che non garantiscono un livello adeguato di protezione.

Con il primo documento sono stati fissati alcuni aspetti procedurali prevedendo,

come auspicato da soggetti interessati, la designazione di un unico interlocutore, ossia di un'autorità di protezione dati che opererebbe quale "*leader*" della valutazione, alla quale tutte le altre autorità interessate dei Paesi Ue dovrebbero far capo per commenti ed osservazioni. La designazione spetterebbe alla società multinazionale, la quale dovrebbe rifarsi ai criteri indicati nel documento, fra i quali la priorità viene data alla considerazione del Paese ove è situata la capogruppo o la sede centrale europea della multinazionale. Le autorità sono libere di accettare o meno tale designazione, sulla base della documentazione prodotta dalla società, eventualmente formulando una contro-proposta.

La procedura prevede, stabilita l'autorità-*leader*, l'elaborazione di una bozza finale di "regole vincolanti nell'impresa" sottoposta alla valutazione congiunta di tutte le autorità interessate, coordinate dall'autorità-*leader*; l'accettazione di tale bozza finale varrebbe come riconoscimento dell'adeguatezza delle norme in essa contenute e, quindi, come autorizzazione al loro impiego.

Contestualmente all'elaborazione del primo documento citato il Gruppo ha prodotto un ulteriore documento (WP 108) che integra e completa il precedente, fornendo indicazioni specifiche sui contenuti delle regole vincolanti nell'impresa. Rifacendosi ai criteri fissati nel giugno del 2003 (documento WP 74, 3 giugno 2003; *cfr. Newsletter* 2-8 giugno 2003), i Garanti europei hanno elaborato una *checklist* che le imprese potrebbero utilizzare per dimostrare che le rispettive "regole vincolanti nell'impresa" rispondono ai principi fissati nella direttiva 95/46/Ce. Ciò concerne, in particolare, la verifica dell'effettiva vincolatività delle regole –sia all'interno del gruppo (rispetto a controllate, collegate, dipendenti e terzi fornitori), sia all'esterno– soprattutto ai fini dell'esercizio dei diritti riconosciuti agli interessati.

Dati dei passeggeri e vettori aerei

Con riguardo al trasferimento dei dati dei passeggeri europei alle autorità doganali di Paesi non appartenenti all'Unione europea, la Commissione europea, con decisione del 14 maggio 2004, n. 2004/535/Ce (*v. Relazione* 2004, p. 260) aveva ritenuto che l'Ufficio statunitense delle dogane e della protezione delle frontiere (*United States Bureau of Customs and Border Protection*, "Cbp") del Ministero della sicurezza interna (*Department of Homeland Security*) sia in grado di offrire un livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei (*Passenger Name Record*, "Pnr") trasmessi dalla Comunità per quanto riguarda i voli con destinazione o in partenza dagli Stati Uniti, in conformità alla Dichiarazione d'impegno del Ministero della sicurezza interna (*Department for Homeland Security*)-Ufficio delle dogane e della protezione delle frontiere (Cbp) dell'11 maggio 2004, che figura in allegato alla decisione medesima.

Secondo il giudizio della Commissione europea i criteri utilizzati dal Cbp per trattare i dati Pnr dei passeggeri, in conformità alla legislazione statunitense e alla Dichiarazione d'impegno dello stesso Cbp, comprenderebbero elementi fondamentali per assicurare un livello di protezione adeguato delle persone fisiche interessate.

Dovendosi attenere a tale valutazione il Garante, il 14 luglio 2005, ne ha dato attuazione ai sensi del Codice, autorizzando il trasferimento fuori dal territorio dello Stato italiano all'Ufficio statunitense delle dogane e della protezione delle frontiere del Ministero della sicurezza interna, da parte dei vettori aerei che assicurano il trasporto di passeggeri con destinazione o in partenza dagli Stati Uniti, dei dati personali contenuti nelle schede nominative dei passeggeri, nella misura in cui tali dati siano stati raccolti e memorizzati nei relativi sistemi informatici di prenotazione, sulla base dei presupposti e in conformità a quanto previsto dalla decisione della Commissione europea sopra citata e alla Dichiarazione di impegno ivi allegata (*Autorizzazione* 14 luglio 2005 [doc. *web* n. 1149808], in *G.U.* 25 luglio 2005, n. 171).

9.6. *Lavoro*

Informativa per la Borsa continua nazionale del lavoro

Nell'ambito delle attività di approfondimento sui profili di interrelazioni tra le norme contenute nel d.lg. n. 276/2003 e le disposizioni in materia di protezione dei dati personali in ambito lavorativo, sono state fornite alcune indicazioni sul testo di informativa predisposto per gli utenti (lavoratori e imprese) della Borsa continua nazionale del lavoro.

L'esame dell'informativa è stato svolto con la collaborazione di Italia lavoro S.p.A., soggetto deputato a fornire il supporto tecnico e strumentale alla Commissione per il raccordo e il coordinamento permanente tra il livello regionale e quello nazionale della Borsa in qualità di segreteria tecnico-organizzativa della stessa (art. 7, comma 4, d.m. 13 ottobre 2004).

Si è rappresentata, in particolare, l'opportunità di elaborare un'informativa che tenesse conto di una pluralità di circostanze:

- il differente ruolo spettante a ciascun titolare del trattamento nel sistema della Borsa continua nazionale del lavoro;
- la necessità di considerare titolari del trattamento esclusivamente i soggetti indicati dall'art. 6 del predetto decreto interministeriale (cioè, il Ministero del lavoro e delle politiche sociali, le regioni e gli operatori pubblici e privati, ad esclusione degli enti previdenziali ed assistenziali ai quali non compete il ruolo di titolari del trattamento dei dati trattati nella Borsa e che, per la peculiare funzione istituzionale rivestita, non possono essere designati quali responsabili del trattamento da uno dei titolari), specificando il ruolo rivestito da alcuni soggetti preposti al trattamento dei dati in nome e per conto dei titolari e, in tale eventualità, provvedendo (se del caso) a designarli quali responsabili del trattamento e ad identificarli, e fornendo agli interessati l'indirizzo dove reperire l'elenco completo, ovvero consentendo l'accesso a tale elenco mediante un *link* ipertestuale nel sito del Ministero del lavoro e degli altri titolari del trattamento;
- la necessità di esplicitare i diritti degli interessati previsti dall'art. 7 del Codice inserendo opportuni riferimenti (indirizzi di posta elettronica o numeri di telefax o di *call center*), utilizzabili per l'esercizio di tali diritti;
- l'esigenza di chiarire, ferma restando la facoltatività dell'iscrizione alla Borsa, quali dati debbano essere conferiti necessariamente e quali, invece, facoltativamente, ai fini dell'iscrizione, esplicitando anche le conseguenze derivanti dal rifiuto al conferimento di tali dati (ai sensi dell'art. 13, comma 1, lett. *b*) e *c*), del Codice).

L'Autorità ha formulato una riserva in ordine alla possibile espressione, anche ai sensi dell'art. 154, comma 1, lett. *g*), del Codice, di pareri eventualmente chiesti sui profili di protezione dei dati personali emersi in tema di trattamenti effettuati mediante la Borsa, rispetto ai quali si è manifestata la necessità di valutazioni più approfondite con tutti i soggetti interessati al suo funzionamento.

Le agenzie per l'impiego

Nell'ambito della collaborazione richiesta da un'associazione rappresentativa (Assores) di alcuni tra i nuovi operatori privati del mercato del lavoro rientranti tra le agenzie per l'impiego introdotte dalla l. n. 30/2003 (e dal d. lg. n. 276/2003), l'Ufficio del Garante ha fornito alcuni chiarimenti sui profili di protezione dei dati personali dei candidati all'instaurazione di rapporti di lavoro subordinato. Si è ribadito che il consenso dell'interessato, ove prescritto, deve essere reso ai sensi degli artt. 23 e ss. del Codice, dal momento che la disciplina in materia di protezione dei dati non riconosce validità ed efficacia al consenso implicito o manifestato per atti concludenti. È stato altresì sottolineato che il consenso al trattamento dei dati "comuni" non è neces-

sario nei casi di cui all'art. 24, comma 1, del Codice (nel caso di specie, lett. *a*) e *b*)). In tal senso, si è richiamata l'interpretazione già fornita dal Garante con il *provvedimento* in materia di annunci di lavoro del 10 gennaio 2002 [doc. *web* n. 1064553].

Nel confermare, per converso, l'obbligo per i titolari del trattamento di fornire agli interessati un'informativa completa degli elementi prescritti dall'art. 13 del Codice (avvalendosi eventualmente delle formule sintetiche già suggerite dal Garante con il citato provvedimento del 2002), è stato confermato l'impegno a valutare, in sede di adozione del codice di deontologia di cui all'art. 111 del Codice, le modalità attraverso le quali i titolari del trattamento potranno rendere un'informativa semplificata (nei casi eventualmente non già contemplati dall'art. 9 d.lg. n. 276/2003) o potrebbero essere esonerati dal relativo obbligo.

Sono state inoltre fornite indicazioni in materia di notificazione al Garante dei trattamenti che le società rappresentate da Assores potrebbero essere tenute ad effettuare a norma dell'art. 37, comma 1, lett. *d*) ed *e*), del Codice e alla luce del *provvedimento* a carattere generale del Garante del 31 marzo 2004 relativo ai casi sottratti all'obbligo di notificazione [doc. *web* n. 852561].

Navigazione in Internet e controllo sui lavoratori

Il Garante si è pronunciato su un ricorso proposto da un lavoratore che lamentava l'illiceità del controllo effettuato dal datore di lavoro sulle navigazioni in Internet (*Provv.* 2 febbraio 2006 [doc. *web* n. 1229854]).

Il datore di lavoro aveva contestato al dipendente, in seguito licenziato, di aver consultato siti a contenuto religioso, politico e pornografico, fornendone l'elenco dettagliato ed allegando alla contestazione disciplinare notificata al lavoratore numerose pagine dei *file* temporanei e dei *cookie* originati sul suo *computer* dalla navigazione in rete avvenuta durante sessioni di lavoro avviate con la *password* del dipendente. Si trattava di informazioni ricavate da pagine *web*, copiate direttamente dalla *directory* intestata al lavoratore, che la società non avrebbe potuto trattare senza averlo informato preventivamente. In secondo luogo, sebbene i dati fossero stati raccolti nel corso di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile, in grado di rivelare ad esempio convinzioni religiose e opinioni sindacali o politiche, potevano essere trattate dal datore di lavoro senza il consenso dell'interessato solo se indispensabili per far valere o difendere un diritto in sede giudiziaria. Tale indispensabilità non è emersa dagli elementi in atti.

È emerso, altresì, un trattamento dei dati relativi allo stato di salute e alla vita sessuale che, a norma del Codice, può essere effettuato senza il consenso dell'interessato solo se necessario per difendere in giudizio un diritto di rango pari a quello dell'interessato della personalità o un altro diritto fondamentale. Anche tale circostanza non è risultata comprovata in atti, dal momento che la società intendeva far valere, invece, diritti legati allo svolgimento del rapporto di lavoro.

L'Autorità ha pertanto vietato alla società l'uso dei dati relativi alla navigazione in Internet del lavoratore, sul presupposto che per contestare l'indebito utilizzo di beni aziendali sarebbe stato proporzionato, nel caso di specie, verificare gli avvenuti accessi a Internet e i tempi di connessione, senza indagare sui contenuti dei siti.

Sistemi di rilevazione biometrica nei luoghi di lavoro

Nel corso dell'anno si è intensificata l'attività dell'Autorità volta alla valutazione della liceità dell'impiego dei sistemi di rilevazione biometrica in specifici contesti e per diverse finalità.

Il Garante ha adottato alcune decisioni a seguito di un formale interpello da parte di alcuni titolari del trattamento, conformemente a quanto stabilito dall'art. 17 del Codice (e dall'art. 20 della direttiva 95/46/Ce). In tale ambito, muovendo dal presupposto che il trattamento di dati biometrici dei lavoratori può risultare in concreto pregiudizievole sul piano del rispetto dei principi di necessità, finalità e proporziona-

lità, sono proseguiti gli approfondimenti iniziati nel 2004 circa l'utilizzo di tecniche di autenticazione biometrica, basate in particolare su impronte digitali.

Un primo caso ha riguardato un'industria di coperture in fibrocemento e metalliche che intendeva implementare un sistema di rilevazione biometrica basato sull'impiego delle impronte digitali dei lavoratori al fine di accertarne la presenza sul luogo di lavoro e di commisurare la retribuzione da corrispondere.

L'impresa intendeva in tal senso prevenire alcune condotte abusive e ovviare allo smarrimento delle tessere magnetiche in uso. Il sistema prevedeva la raccolta dell'impronta di ciascun dipendente e la sua trasformazione in un codice numerico (*template*) poi memorizzato, senza cifratura, nella banca dati aziendale. A ciascun ingresso in azienda i lettori elettronici avrebbero rilevato l'impronta e confrontato il codice da questa ricavato con il *template* previamente memorizzato.

Dall'istruttoria non sono emersi elementi che potessero giustificare la richiesta di introdurre la rilevazione di dati biometrici (come, ad esempio, la necessità di limitare accessi ad aree dell'azienda che richiedono *standard* di sicurezza particolarmente elevati in ragione di specifiche circostanze o attività svolte). Il trattamento è stato pertanto vietato in quanto sproporzionato e non necessario rispetto allo scopo perseguito (*Provv.* 21 luglio 2005 [doc. *web* n. 1150679]). Rispetto alla finalità specifica il Garante ha infatti ritenuto l'uso di dati biometrici eccessivamente invasivo della sfera personale e della libertà individuale dei lavoratori in quanto, pur rientrando il controllo sull'esecuzione della prestazione lavorativa tra le legittime facoltà del datore di lavoro (art. 2094 c.c.), anche attraverso la predisposizione di strumenti di controllo del rispetto dell'orario di lavoro da parte dei lavoratori, per il raggiungimento di tale scopo possono essere adottate altre tecniche più rispettose del principio di proporzionalità ed ugualmente rigorose.

Il trattamento è risultato sproporzionato anche sul piano delle modalità tecniche prefigurate. In luogo della proposta centralizzazione in una banca dati aziendale dei codici identificativi generati dall'esame dell'impronta, il Garante ha osservato che sarebbe stato preferibile una memorizzazione del *template* su un supporto digitale da assegnare al lavoratore e tale da rimanere nella sua esclusiva disponibilità, in modo da prevenire maggiori ripercussioni per i diritti individuali in caso di violazione delle misure di sicurezza, di accesso di persone non autorizzate o comunque di abuso delle informazioni memorizzate.

La stessa informativa predisposta ai sensi dell'art. 13 del Codice è apparsa incompleta rispetto al trattamento ipotizzato: le dichiarazioni rese dalla società circa la libertà accordata ai lavoratori di aderire o meno al sistema di controllo delle presenze basato sull'utilizzo di dati biometrici e all'adozione di strumenti alternativi di rilevazione per i lavoratori impossibilitati, per ragioni fisiche, a registrare le presenze mediante l'impiego del sistema biometrico, non hanno trovato conferma nell'informativa predisposta, secondo la quale il conferimento dei dati, ivi compresi i dati biometrici, avrebbe avuto natura obbligatoria.

Un diverso caso ha riguardato una società fornitrice di tecnologie per la difesa nel settore avionico ed elettronico, che ha presentato all'Autorità una richiesta di verifica preliminare relativa al trattamento di dati biometrici di un numero ristretto di dipendenti al fine di controllarne gli accessi ad un'area aziendale circoscritta. L'impiego delle impronte digitali dei lavoratori interessati era reputato dalla società necessario per identificare in modo certo i soggetti abilitati all'accesso in un'area riservata, nella quale veniva sviluppato un particolare programma avionico rilevante nel settore della difesa, per la cui realizzazione è richiesto un ambiente conforme a *standard* di sicurezza specifici ed elevati richiesti dalla Nato.

Il sistema proposto, basato sulla raccolta di impronte digitali mediante apparecchiature dotate di lettore di impronte digitali e di un apposito *software*, prevedeva che i dati venissero trasformati in un codice numerico (*template*) utilizzato esclusivamente per la raccolta e il successivo trattamento ai fini predetti.

Il trattamento di dati oggetto di verifica preliminare è stato ritenuto lecito alla luce delle specifiche finalità perseguite nel contesto esaminato, degli accorgimenti già adottati dalla società e di talune misure prescritte dal Garante in relazione alle concrete modalità di identificazione biometrica (*Provv.* 23 novembre 2005 [doc. *web* n. 1202254]). I dati trattati sono risultati pertinenti e non eccedenti rispetto alla finalità perseguita in quanto riferiti (non alla generalità dei dipendenti, ma soltanto) ad un numero ridotto di lavoratori (in possesso di nulla osta di sicurezza ed impiegati in attività che comportano la necessità di trattare informazioni rigorosamente riservate).

L'Autorità ha però prescritto alla società di predisporre un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il *template* memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati, senza creare un archivio centralizzato; ciò dotandosi, ove ritenuto opportuno al fine di identificare con maggiore certezza gli interessati, di un dispositivo idoneo a registrare nel sistema informativo aziendale dedicato all'archiviazione degli accessi all'area riservata altre informazioni personali (anche in forma di codice) necessarie ad identificare univocamente i lavoratori che vi accedono.

Ulteriori casi di impiego di tecniche di rilevazione biometriche nei luoghi di lavoro (attualmente al vaglio dell'Autorità) riguardano, da un lato, la verifica preliminare richiesta da tre società svolgenti attività industriale di carattere molitorio e che intendono porre in essere trattamenti finalizzati alla rilevazione delle presenze e al controllo accessi dei propri dipendenti basato sull'impiego delle loro impronte digitali; dall'altro, la sperimentazione di un sistema di riconoscimento facciale presso l'Aeroporto di Fiumicino "Leonardo da Vinci". A tale proposito, a seguito di segnalazioni provenienti da alcuni interessati, sono stati svolti accertamenti ispettivi che hanno evidenziato come il sistema sia stato installato in via sperimentale per soli 4 mesi presso un varco del *terminal* adibito al transito del personale di *staff*, utilizzato per accedere all'interno di aree sterili dell'aeroporto. I soggetti coinvolti nella sperimentazione (oltre 3.000 operatori aeroportuali) sono stati iscritti al programma su indicazione delle compagnie aeree e delle altre società interessate dalle quali dipendevano. Al fine di consentire la sperimentazione, la società di gestione dell'aeroporto ha messo a disposizione proprio personale addetto alle fasi di registrazione (*enrollment*) dei dati biometrici (avvenuta su *smart-card*, utilizzate come supporto per la memorizzazione della geometria del volto) e di controllo al varco di riconoscimento biometrico.

9.7. *Condomini*

Trattamento dei dati personali nell'amministrazione dei condomini

Il Garante, muovendo dalle problematiche rilevate dall'esame di segnalazioni e quesiti, tenendo conto di provvedimenti adottati in precedenza (in buona parte, in sede di decisione su ricorso) e in vista dell'adozione di un proprio provvedimento, ha avviato una consultazione pubblica in tema di trattamento dei dati nell'ambito delle attività connesse alla gestione dei condomini, chiedendo altresì alle associazioni di categoria interessate (in particolare, associazioni di condomini, amministratori condominiali e conduttori), agli operatori di settore e ai cittadini di far pervenire osservazioni (con riguardo ai profili relativi alla tipologia di dati trattati, alla loro circolazione all'interno del condominio e all'esercizio del diritto d'accesso), e

invitando le medesime associazioni a tenere conto delle considerazioni, di natura generale, idonee a compendiare i precedenti orientamenti sul punto, contenute in un documento di sintesi a tal fine reso disponibile sul sito *web* del Garante.

Sono pervenute all'Autorità 75 comunicazioni di contenuto eterogeneo (richieste di chiarimenti, segnalazioni, quesiti, osservazioni), unitamente a quelle inviate dalle associazioni di categoria.

Tali comunicazioni hanno preso prevalentemente in considerazione i seguenti profili:

- la questione della titolarità del trattamento nell'ambito della gestione condominiale;
- la tipologia dei dati trattati (in particolare, dall'amministratore nello svolgimento del proprio ufficio), tra i quali vengono indicati:
  - i dati inerenti al condominio complessivamente inteso quale ente di gestione (ad esempio, rispetto al conto corrente condominiale, ai contratti per la fornitura di beni e somministrazione di servizi; dati sul consumo ed importi di utenze complessivamente intestate al condominio);
  - i dati personali dei singoli partecipanti al condominio, nei limiti delle informazioni personali raccolte ed utilizzate per le finalità riconducibili alla disciplina civilistica (informazioni relative ai dati anagrafici e ai recapiti degli altri condomini, quote millesimali attribuite a ciascuno di essi, altre informazioni utili a determinare i diritti o gli oneri dei singoli condomini in relazione alle aree comuni);
- il trattamento dei dati relativi a soggetti diversi dai partecipanti al condominio (inquilini, coabitanti e conduttori);
- la circolazione in varie forme, verso terzi, di dati relativi alla gestione condominiale: a) partecipazione all'assemblea da parte di tecnici e professionisti; b) deleghe di voto in assemblea; c) dati conoscibili dal conduttore (anche mediante invio del verbale di assemblea); d) diffusione dei dati (affissione dati personali in bacheche condominiali);
- le problematiche afferenti alle misure di sicurezza;
- trattamento dati personali, sensibili e giudiziari, relativi al rapporto di lavoro con dipendenti e alla disciplina sull'abbattimento delle barriere architettoniche (l. n. 13/1989);
- la gestione della documentazione sanitaria per infortuni in aree condominiali.