9 Attività economiche

9.1. *Credito*

Accesso ai dati personali e accesso alla documentazione bancaria

Continuano a pervenire all'Autorità numerose segnalazioni concernenti il rapporto tra diritto di accesso ai dati personali detenuti da istituti di credito, disciplinato dagli artt. 7 e seguenti del Codice, e il diritto di ottenere copia della documentazione bancaria ai sensi dell'art. 119 d.lg. n. 385/1993 (Testo unico in materia bancaria e creditizia), correlato al profilo relativo al rimborso spese chiesto dalle banche ai sensi dello stesso art. 119 per rendere disponibile la documentazione. Nelle risposte inviate dall'Ufficio del Garante è stata ribadita la posizione, già espressa dall'Autorità in una nota inviata alla Banca d'Italia (*Nota* 6 agosto 2004, in *Relazione* 2004, p. 60), con la quale si è precisato il differente ambito di applicazione delle due norme e la conseguente competenza del Garante a pronunciarsi, in termini generali, sulle sole richieste di accesso a dati personali formulate ai sensi del menzionato art. 7 del Codice. Per tale ragione, la richiesta volta a conoscere tali dati personali non può "trasformarsi" in una pretesa del richiedente ad ottenere direttamente, sempre e comunque, copia integrale della documentazione che contenga i dati medesimi.

Rimessa interbancaria diretta

Un altro aspetto, in relazione al quale si sono registrate alcune segnalazioni, ha riguardato il trattamento non autorizzato di dati personali riferiti a clienti (in particolare, delle loro coordinate bancarie). Un cliente ha, ad esempio, contestato l'addebito di una bolletta telefonica tramite rapporti interbancari diretti (R.i.d.), pur non avendo prescelto tale forma di pagamento e non avendo fornito le proprie coordinate bancarie. I titolari del trattamento non hanno fornito prova della circostanza che il cliente fosse stato altresì informato preventivamente dell'utilizzo dei dati con la procedura in esame e sono state fornite alcune prescrizioni a tutela della libertà di scelta del cliente in relazione alle modalità di pagamento.

Trattamenti effettuati nell'ambito dei sistemi di rilevazione creditizia

Dal 1° gennaio 2005 ha trovato applicazione il "codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti" (sottoscritto il 12 novembre 2004 da tutte le associazioni rappresentative del settore e da varie associazioni di consumatori): esso prevede regole specifiche alle quali gli operatori del settore creditizio e finanziario devono attenersi in relazione ai trattamenti di dati personali relativi a contratti di finanziamento.

Come ricordato in precedenti relazioni, per lungo tempo le *cd.* centrali rischi private hanno operato in assenza di un quadro regolamentare. Al di là della conseguente incertezza dal punto di vista dell'operatività di questi sistemi, per ragioni diverse è risultato elevato il contenzioso in materia nei primi anni di applicazione della disciplina di protezione dei dati personali (accentuato dagli effetti negativi che ha sull'accesso al credito l'avvenuta segnalazione in dette centrali). Ciò, in ragione della scarsa trasparenza dei tempi di conservazione dei dati (reputati eccessivamente lunghi, specie in presenza di segnalazioni dovute a meri ritardi nei pagamenti o ad inadempimenti di importo contenuto), a causa della qualità dei dati trattati, non sempre esatti o aggiornati, oltre che per il mancato (o tardivo) riscontro all'esercizio del diritto d'accesso da parte degli interessati.

L'adozione del codice di deontologia e buona condotta da parte degli operatori

del settore (preceduta da una copiosa serie di decisioni su ricorsi proposti *ex* art. 145 del Codice) ha perciò rappresentato una tappa significativa nell'attività svolta dal Garante in questo ambito assai delicato: essa ha determinato l'emersione del fenomeno della referenziazione creditizia, specie grazie alla formulazione di un'informativa chiara agli interessati da parte dei soggetti partecipanti a detti sistemi d'informazione, ed ha determinato una più puntuale attenzione alla qualità delle informazioni trattate ai fini della valutazione del rischio di credito, unitamente alla definizione dei tempi massimi di conservazione delle medesime.

Il codice deontologico ha previsto una serie di misure a carico degli operatori del settore da adottare in fasi successive, nel corso della prima metà del 2005. Tra di esse figuravano la riduzione dei tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo positivo, la costituzione di un organismo di controllo con la partecipazione di rappresentanti delle associazioni consumeristiche, l'invio al Garante delle informazioni e della documentazione necessaria per consentire il controllo sulla corretta attuazione delle disposizioni contenute nel Codice e l'integrazione dell'informativa fornita agli interessati, contenente le informazioni non comprese nelle informative rese precedentemente.

L'attività svolta nel corso dell'anno dall'Autorità in questo settore ha, quindi, richiesto un attento esame dell'operato dei nuovi sistemi di informazioni creditizie (Sic) allo scopo di valutare sia la progressiva attuazione delle misure previste, sia i primi problemi applicativi. In questa cornice si è svolta, nella seconda parte dell'anno, un'estesa attività di accertamento in loco presso i gestori dei principali sistemi, che ha avuto ad oggetto la verifica della conformità dei trattamenti concretamente posti in essere, rispetto alla disciplina di protezione dei dati personali come integrata dalle disposizioni di natura deontologica. L'attività di accertamento si è protratta presso i gestori di servizi di comunicazione elettronica nei primi mesi del 2006, in vista dei provvedimenti calendarizzati per la prima parte del 2006.

Con riguardo alla tematica dei tempi di conservazione, l'art. 13, comma 4 del codice deontologico prevedeva invece che, in sede di prima applicazione delle disposizioni contenute nell'art. 6 del medesimo codice, i gestori riducessero ad un termine non superiore a trentasei mesi i tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo "positivo" (relative, cioè, all'avvenuta conclusione positiva del rapporto contrattuale o al diligente adempimento degli obblighi contrattuali in corso). In tempi successivi, l'organo di controllo previsto dall'art. 13, comma 7, del codice deontologico avrebbe valutato, alla luce dell'esperienza maturata, se fosse giustificato il mantenimento del termine più lungo, e il Garante, su richiesta del predetto organismo o di propria iniziativa, avrebbe dovuto indicare il termine da osservare. A questo proposito, con avviso pubblicato in *Gazzetta Ufficiale* 6 marzo 2006, n. 54, il Garante ha infine disposto che i dati personali relativi ad informazioni creditizie di tipo positivo possono continuare ad essere conservati nei sistemi di informazioni creditizie per un termine non superiore a trentasei mesi (anziché per il più breve termine di ventiquattro mesi come prefigurato dall'art. 6, comma 6, del codice deontologico).

Contributo-spese per l'accesso ai dati Sic

Con *deliberazione* n. 15/2004 il Garante aveva riconosciuto, a favore di una società che gestisce un Sic, la possibilità di richiedere contributi-spese in casi ulteriori rispetto a quelli già previsti, in via generale, dalla *deliberazione* n. 14/2004 ([doc. *web* n. 1104892], in *G.U.* 8 marzo 2005, n. 55). La deliberazione era espressamente valida solo per il 2005, con riserva di riesaminare la questione entro lo stesso anno e di confermare, o meno, in tale sede, la previsione di detto contributo.

Alla fine del 2005 la società ha rinnovato la richiesta, unitamente alle analoghe

richieste di altre società che gestiscono sistemi di informazione creditizia. Il Garante ha ritenuto che non sussistessero i presupposti per adottare una deliberazione analoga. Sono risultate, infatti, esaurite le ragioni che avevano condotto a tale determinazione, individuate nell'effettuazione di investimenti di varia natura per semplificare le procedure di riscontro all'esercizio del diritto d'accesso. Il contributo potrà comunque essere richiesto dai titolari nelle misure indicate in via generale dalla deliberazione n. 14/2004 per tutte le categorie di titolari del trattamento.

Sistemi di rilevazione di impronte digitali ed immagini per accesso a banche

Già in passato il Garante ha affrontato in alcuni provvedimenti il tema relativo all'impiego da parte delle banche di sistemi di rilevazione delle impronte digitali in associazione con sistemi di videosorveglianza (*cfr.*, soprattutto, *Provvedimenti* 28 settembre 2001 [doc. *web*. n. 39704] e 29 aprile 2004 [doc. *web*. n. 1003482]). In considerazione delle segnalazioni provenienti da parte di cittadini che, in presenza di talune circostanze, contestavano le modalità di accesso ad istituti bancari e in ragione delle numerose richieste di nuove installazioni provenienti da banche che invocavano una recrudescenza di fenomeni criminali –circostanza rappresentata anche dall'Associazione bancaria italiana–, il Garante è tornato a pronunciarsi in materia.

Con *provvedimento* del 27 ottobre 2005 [doc. *web* n. 1246675] (in *G.U.* 22 marzo 2006, n. 68 ; *cfr*. anche *Provv.* 2 marzo 2006 [doc. *web* n. 1248850], pubblicato nella stessa *G.U.* 22 marzo 2006, n. 68), il Garante, ribadendo il proprio indirizzo –contrario all'uso generalizzato di sistemi che associno immagini e impronte digitali–, ha individuato le misure e gli accorgimenti che, a garanzia degli interessati, devono essere adottati dagli istituti di credito che intendano avvalersi di sistemi di rilevazione dell'impronta digitale in associazione a sistemi di videosorveglianza. Secondo il provvedimento, che ha tenuto conto delle novità sopravvenute con l'entrata in vigore del Codice (in particolare, gli artt. 17, 24, comma 1, lett. *g*) e 154, comma 1, lett. *c*)) e dei principi generali già enunciati nei citati *provvedimenti* del 28 settembre 2001 e 29 aprile 2004, è lecito installare apparecchiature che consentano l'identificazione delle persone attraverso la combinazione di telecamere e di sistemi per la raccolta dell'immagine delle impronte digitali, solo in presenza di condizioni di effettivo rischio (*ad es.*, con riguardo a sportelli siti in aree ad effettiva alta densità criminale, oppure in aree isolate o nella prossimità di "vie di fuga") e per l'esclusiva finalità di incrementare il grado di sicurezza di beni e persone.

Se non sono rispettati i principi di necessità e di proporzionalità il trattamento dei predetti dati non è lecito. Misure articolate devono essere comunque adottate affinché il trattamento sia conforme ai principi di protezione dei dati personali. In particolare:

- la banca, prima che i dati siano rilevati (e, comunque, prima dell'accesso del cliente all'interno della propria sede), deve fornire agli interessati un'informativa sintetica, ma chiara, relativa alla presenza di sistemi di raccolta di impronte digitali e di immagini; informativa che dovrà essere integrata da un'altra, più ampia, informativa esposta all'interno dei locali della banca;
- ai clienti deve essere comunque consentito l'accesso alla banca con modalità alternative, senza apporre le proprie impronte digitali. Ciò, sia disabilitando (temporaneamente) il sistema di rilevazione delle impronte, sia utilizzando accessi alternativi (in tal caso si possono adottare opportune cautele in relazione all'accesso del cliente, quali, ad esempio, la richiesta di esibizione di un suo documento di identificazione);
- le immagini e le impronte digitali devono essere cifrate prima della loro registrazione in un archivio. Il provvedimento ha previsto che il processo crittografico sia garantito dalla figura del "vigilatore dei dati", un soggetto indipendente, anche esterno alla banca, depositario delle chiavi crittografi-

che idonee a decifrare le informazioni conservate. Ai dati "in chiaro" possono accedere soltanto l'autorità giudiziaria e la polizia;

- i dati relativi alle immagini e alle impronte digitali devono essere cancellate automaticamente, salvo quanto disposto per specifici motivi di giustizia o a seguito della richiesta di un interessato, trascorso un periodo non superiore ad una settimana.

Anche al fine di agevolare un'eventuale attività di verifica preliminare, come pure (più in generale) di controllo da parte dell'Autorità, il provvedimento prevede che le banche, le quali intendano intraprendere trattamenti del tipo qui descritto, o che abbiano già installato sistemi di rilevazione dell'immagine e dell'impronta digitale, debbano comunicare detta circostanza al Garante inviando una specifica richiesta per via telematica compilando il modello reso disponibile sul sito *web* dell'Autorità.

Identificazione della clientela presso istituti bancari e postali

Tenendo conto di numerose segnalazioni, il Garante è intervenuto per valutare la conformità, rispetto alla normativa in materia di protezione dei dati personali, della prassi seguita da istituti di credito ed uffici postali che, nell'effettuare operazioni bancarie, finanziarie o postali (*ad es.*, ordinarie operazioni di versamento, pagamenti e altre disposizioni impartite dalla clientela, presentazione per il pagamento di assegni o vaglia postali), identificano clienti mediante richiesta di esibizione di un valido documento di riconoscimento e acquisendone talvolta la relativa copia fotostatica (in particolare, in caso di soggetti non correntisti o comunque non conosciuti dal personale di filiale) (*Provv.* 27 ottobre 2005, [doc. *web* n. 1189435]).

Dopo aver rilevato che le operazioni di identificazione implicano un trattamento di dati personali –che va conformato anch'esso ai principi di liceità, pertinenza e non eccedenza rispetto alle finalità perseguite (art. 11 del Codice)– il Garante ha osservato che è necessario, per valutare la fattispecie, distinguere tra la necessità generale di identificare la persona e le modalità con cui ciò avviene.

L'identificazione del soggetto che effettua una determinata operazione risulta a volte prescritta da una disposizione normativa (si pensi, ad esempio, all'art. 2, comma 14, d.l. 30 settembre 2005, n. 203, a modifica dell'art. 7 d.P.R. 29 settembre 1973, n. 605, oppure all'art. 45 d.P.R. 28 dicembre 2000, n. 445, relativo alle modalità per identificare i cittadini da parte di organi della pubblica amministrazione e di gestori di pubblici servizi o, ancora, alle vigenti disposizioni in materia di riciclaggio), mentre può essere altre volte necessaria per eseguire obblighi derivanti dal contratto o per adempiere a specifiche richieste precontrattuali dell'interessato (art. 24, comma 1, lett. *a*) e *b*), del Codice). In tali ipotesi, fatta salva l'osservanza dell'obbligo di informativa (fornita anche *una tantum* al cliente), non è necessario richiedere il consenso dell'interessato.

Le modalità con le quali avviene l'identificazione, in ossequio al principio di proporzionalità, devono tener conto delle circostanze di fatto: fuori dai casi in cui espresse disposizioni normative stabiliscano precise modalità, la banca o l'ufficio postale ha l'onere di verificare l'identità dell'interessato basandosi su idonei elementi di valutazione, quali, ad esempio, la conoscenza personale, la consultazione di atti e documenti acquisiti in precedenza, anche in sede di instaurazione del rapporto, ovvero l'esibizione di un documento di riconoscimento, provvedendo se del caso ad annotarne gli estremi.

La richiesta di produrre, anche per via telematica, la copia di un documento di riconoscimento e la sua conservazione presso la filiale possono ritenersi giustificate solo quando si rinvenga una disposizione normativa che preveda espressamente l'acquisizione e la conservazione temporanea di tale copia, oppure quando la banca o l'ufficio postale debba poter dimostrare di aver identificato l'interessato con modalità più accurate, tenendo conto del particolare contesto e delle operazioni da

svolgere. In questi ultimi casi può rientrare anche quello del portatore "non conosciuto" di un assegno (o di un vaglia): in tale ipotesi, l'acquisizione del relativo documento è da ritenersi legittima considerata la responsabilità della banca o dell'ufficio postale in relazione ai pagamenti che vanno effettuati, con la necessaria diligenza, solo al creditore (*cfr.* anche l'art. 1189 c.c. e gli artt. 43 e 86 r.d. 21 dicembre 1933, n. 1736).

Il Garante ha affermato conclusivamente che il trattamento delle informazioni raccolte a fini di identificazione risulta lecito, pertinente e non eccedente se effettuato nei termini sopra riassunti, i quali trovano riscontro nelle disposizioni dell'ordinamento che prevedono già la necessità di conservare copia di un documento da esibire. In applicazione del principio della pertinenza e di non eccedenza nel trattamento dei dati occorre altresì evitare di acquisire più volte copie di documenti già disponibili agli atti e, comunque, di utilizzarle ad altri scopi. Infine, gli istituti bancari e gli uffici postali devono assicurare che l'accesso alle informazioni sia consentito unicamente nelle ipotesi indicate e solo da chi ne abbia titolo, evitando, in ciascuna fase, ogni inutile comunicazione di dati personali anche nello svolgimento di operazioni allo sportello.

9.2. *Assicurazioni*

Accesso agli atti assicurativi e protezione dei dati

Nell'ambito del settore assicurativo, si ripropone con accresciuta frequenza il tema dell'accesso alla documentazione del procedimento di liquidazione dei danni ai sensi dell'art. 12-*ter* l. 24 dicembre 1969, n. 990 (introdotto dall'art. 3 l. 5 marzo 2001, n. 57; *v.* oggi l'art. 146 d.lg. 7 settembre 2005, n. 209, recante il Codice delle assicurazioni private). Tale disciplina risponde alla specifica esigenza di garantire al soggetto assicurato un rapporto trasparente con la compagnia assicuratrice, conferendo allo stesso la possibilità di controllare e verificare i singoli passaggi del procedimento di liquidazione, a conclusione dei procedimenti di valutazione, constatazione e liquidazione dei danni.

A fronte di numerose segnalazioni relative alla possibile interferenza tra la citata disciplina di settore e quella sulla protezione dei dati personali, è stato ribadito in più occasioni l'orientamento già espresso in materia dal Garante (*Provv.* 8 maggio 2001 [doc. *web* n. 39284]) secondo cui la disposizione contenuta nel predetto art. 12-*ter* riconosce un particolare diritto d'accesso alla documentazione, distinto rispetto al diritto di accesso ai dati personali previsto dal Codice, confermando la piena compatibilità tra le due discipline. L'Autorità ha nuovamente distinto chiaramente l'esercizio del diritto di accesso ai dati personali (di cui all'art. 7 del Codice), che può essere esercitato –limitatamente ai dati personali relativi all'interessato– in ogni momento, dal diritto degli assicurati e dei danneggiati ad accedere *"agli atti a conclusione dei procedimenti di valutazione, contestazione e liquidazione dei danni che li riguardano"*, per il quale le sopra menzionate disposizioni normative di rango primario in materia assicurativa (cui è stata data attuazione con il d.m. 20 febbraio 2004, n. 74) stabiliscono, parimenti, precisi limiti temporali a garanzia degli interessati.

La diversa qualificazione dell'istanza da parte del soggetto interessato risulta idonea ad individuare la disciplina di volta in volta applicabile in quanto, se la richiesta di accesso concerne dati personali dell'interessato, troveranno applicazione gli artt. 7 e 8 del Codice e la conseguente possibilità, in caso di mancato o inidoneo riscontro da parte del titolare del trattamento, di adire l'autorità giudiziaria ordinaria o di presentare ricorso al Garante ai sensi degli artt. 145 e ss. del Codice. Qualora, invece, l'oggetto dell'accesso riguardi la documentazione relativa al procedimento di liquidazione

del danno, opereranno i limiti ed i presupposti previsti dalla legge n. 57/2001(ora dal Codice delle assicurazioni private) e dal citato regolamento di attuazione.

A questo proposito è opportuno ricordare che, qualora entro sessanta giorni dalla ricezione della richiesta l'assicurato o il danneggiato non sia messo in condizione da parte della compagnia di assicurazione di prendere visione degli atti richiesti, il medesimo può rivolgersi all'Isvap per vedere garantito il proprio diritto (art. 4, comma 4, d.m. 20 febbraio 2004, n. 74).

Il richiamato orientamento del Garante ha trovato ulteriore conferma alla luce del nuovo testo dell'art. 146 del Codice delle assicurazioni private che, nel disciplinare il diritto degli assicurati e dei danneggiati ad accedere agli atti del procedimento di liquidazione, ha chiarito il rapporto con l'esercizio del diritto di accesso ai dati personali dell'interessato, facendo appunto salvo *"quanto previsto per l'accesso ai singoli dati personali dal codice in materia di protezione dei dati personali"* (comma 1). La disposizione in esame ha inoltre stabilito la non gratuità del diritto di accesso agli atti e ai documenti assicurativi (comma 3) ed ha introdotto, altresì, maggiori limitazioni all'esercizio di tale diritto (che "*non è consentito quando abbia ad oggetto atti relativi ad accertamenti che evidenziano indizi o prove di comportamenti fraudolenti"*; la norma prevede, inoltre, la sospensione del diritto in caso di pendenza di controversia giudiziaria tra l'impresa ed il richiedente). Resta salva, nei casi di preclusione del diritto di accesso ai documenti, la facoltà di esercitare l'accesso ai propri dati personali *ex* art. 7 del Codice, nei limiti dell'art. 8, comma 2, lett. *e*).

Dati sensibili e assicurazioni

Sempre in ambito assicurativo, ulteriori prescrizioni hanno riguardato segnalazioni e quesiti relativi all'accesso alle perizie medico-legali, di regola redatte dai medici fiduciari delle compagnie assicurative. In conformità all'opinione già espressa in passato in una pluralità di decisioni (*Provv.* 8 maggio 2001 [doc. *web* n. 39284], e *Provv.* 20 marzo 2002 [doc. *web* n. 1063450]), nel dare riscontro alle numerose segnalazioni che continuano ad essere inviate all'Autorità è stata confermata la possibilità di esercitare in tale ambito i diritti previsti dall'art. 7 del Codice, rivolgendosi direttamente al titolare o al responsabile del trattamento per ottenere l'accesso ai dati, nei limiti stabiliti dall'art. 8, comma 4.

È stato altresì precisato, in conformità con una precedente pronuncia (*cfr. Provv.* 28 dicembre 2000 [doc. *web* n. 40647] in materia di accesso alle informazioni contenute nella documentazione bancaria), che il diritto di accesso comporta l'obbligo per il titolare del trattamento di estrarre i dati riferiti all'interessato e di trasporli, se vi è richiesta, su un supporto cartaceo o informatico; non è invece attribuito all'interessato il diritto di ottenere "copia integrale" della documentazione contenente i dati personali, salvo che risulti particolarmente difficoltosa l'estrazione dei dati dai medesimi atti o documenti e non sia parimenti possibile la loro trasmissione per via telematica.

Maggiori problemi sembra invece comportare il caso della richiesta, rivolta sempre alla compagnia assicuratrice, di copia della perizia medico-legale avente ad oggetto i dati sanitari relativi ad un terzo (*ad es.*, la persona danneggiata da un sinistro): in tale ipotesi, trattandosi di un caso di comunicazione di dati idonei a rivelare lo stato di salute di un terzo, trova applicazione la disciplina prevista dall'art. 26, comma 4, lett. *c*), del Codice –che ammette il trattamento dei dati sensibili senza il consenso dell'interessato, previa autorizzazione del Garante, in presenza dell'esigenza di esercizio del diritto di difesa, purché il diritto che si intenda difendere sia di "rango almeno pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile" (*Provv.* 9 luglio 2003 [doc. *web* n. 29832]).

Nell'ambito dell'attività riguardante il settore assicurativo è stata esaminata una

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.

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

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.

9

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]).

9

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).

9

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-

9

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.

10 Libere professioni

10.1. *Attività forense. Ordini e collegi professionali*

Nell'ottica del rafforzamento dell'attenzione del Garante e dell'incidenza della sua azione nel mondo delle libere professioni, con particolare riferimento all'attività forense, e nel variegato ambito di operatività dei concessionari di pubblici servizi, l'Autorità ha istituito con deliberazione del 15 dicembre 2005 un'apposita unità organizzativa di primo livello denominata "Unità attività forense, ordini professionali e pubblici servizi", con decorrenza operativa dal 1° gennaio 2006. A tale unità è stato assegnato il compito di curare l'applicazione del Codice rispetto ai trattamenti di dati personali relativi all'attività degli ordini professionali e all'attività forense, nonché a quelli inerenti ai concessionari di pubblici servizi.

Tra i primi obiettivi che l'Autorità intende raggiungere in proposito a partire dal 2006 vi è quello di riavviare i lavori del codice di deontologia e buona condotta previsto dall'art. 135 del Codice, relativo ai trattamenti di dati personali effettuati da investigatori privati e liberi professionisti, in relazione ad investigazioni difensive e a trattamenti effettuati per far valere o difendere un diritto in giudizio.

11 Concessionari di pubblici servizi

11.1. *Servizi di riscossione tributi*

Dichiarazione stragiudiziale

Negli anni passati, intervenendo a seguito di numerosi quesiti, segnalazioni e ricorsi, l'Autorità aveva giudicato illecita la prassi, propria di alcune società concessionarie del servizio per la riscossione dei tributi, consistente nel richiedere a terzi informazioni personali sul contribuente, in modo da ottenere dichiarazioni stragiudiziali attestanti l'esistenza di crediti del contribuente su cui rivalersi; ciò, in quanto nessuna previsione legislativa o regolamentare attribuiva alle società concessionarie il potere di effettuare questo tipo di trattamento.

La legge finanziaria 2005 ha introdotto, in materia, l'istituto della "dichiarazione stragiudiziale" (art. 1, comma 425, l. n. 311/2004), sulla base della quale il concessionario del servizio di riscossione dei tributi risulta ora legittimato a chiedere ai debitori del soggetto iscritto a ruolo di indicare, per iscritto, le cose e le somme da essi dovute allo stesso soggetto, anche solo in modo generico. Nel più volte richiamato *provvedimento* del 25 maggio 2005 [doc. *web* n. 1131826], il Garante ha affermato al riguardo la necessità di verificare il rispetto del principio di pertinenza e non eccedenza e di assicurare che la competente amministrazione impartisca ai concessionari idonee istruzioni, a norma di legge, per i casi in cui si ritenga di dover ricorrere a tale strumento, prevedendo che il concessionario –oltre ad informare l'interessato sul trattamento dei dati– fornisca allo stesso una comunicazione preventiva della possibilità che, in caso di mancato pagamento, verrà acquisita una dichiarazione stragiudiziale prima di procedere al pignoramento presso terzi, utilizzando tale strumento solo dopo aver documentato l'impossibilità di procedere altrimenti alla riscossione del credito. Dovrà essere altresì verificato su base casistica, anche in relazione all'importo dovuto, se le cose e le somme dovute dai debitori del soggetto iscritto a ruolo debbano essere indicate dal terzo in modo generico oppure puntuale, indicando chiaramente nella richiesta il dettaglio delle informazioni richieste e la facoltatività o meno della risposta.

Relativamente a questo aspetto sarà peraltro necessario prendere in considerazione la riforma in materia di servizio nazionale della riscossione introdotta dalla legge finanziaria per il 2006 (l. n. 266/2005, in *G.U.* 29 dicembre 2005, n. 302, *S.O.* n. 211), che ha previsto la costituzione, da parte dell'Agenzia delle entrate e dell'Inps, della società Riscossione S.p.A.

Tarsu

L'Autorità è intervenuta, a seguito di una segnalazione, per valutare la liceità del trattamento di dati personali previsto ai fini del controllo del pagamento della tassa sui rifiuti solidi urbani (Tarsu). Al riguardo, il Garante ha osservato che la normativa di settore riconosce ai comuni, al fine di accertare e controllare il pagamento della citata tassa, la possibilità di invitare direttamente il contribuente ad esibire o trasmettere atti e documenti e di inviare questionari relativi a dati e notizie di carattere specifico, con invito a restituirli compilati e firmati (art. 11, comma 3, d.lg. 30 dicembre 1992, n. 504; art. 73, comma 1, d.lg. 15 novembre 1993, n. 507). Per lo svolgimento di tale attività, i comuni possono peraltro avvalersi legittimamente, in conformità alle disposizioni in materia di protezione dei dati personali, della collaborazione di soggetti privati (*Nota* 6 dicembre 2005).

12 Rapporto di lavoro e previdenza

12.1. *Rapporti di lavoro in ambito pubblico*

Accesso ai dati personali in ambito lavorativo

L'Autorità è intervenuta in numerose occasioni rispetto all'esercizio del diritto di accesso dei lavoratori ai propri dati personali.

Nell'esaminare due ricorsi concernenti richieste volte a conoscere i dati personali conservati in qualsiasi forma dal datore di lavoro, il Garante ha nuovamente precisato che l'esercizio del diritto di accesso consente all'interessato di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione in forma intelligibile dei dati personali detenuti dal titolare del trattamento; non permette, invece, l'accesso diretto e indiscriminato a documenti ed intere tipologie di atti, ovvero la creazione di documenti inesistenti negli archivi, oppure la loro aggregazione innovativa secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia (fotostatica o autenticata) dei documenti detenuti (*Provv.* 16 giugno 2005 [doc. *web* n. 1149999]).

Nel fornire riscontro alla richiesta, il titolare del trattamento deve comunicare solo i dati personali richiesti ed effettivamente detenuti e non è tenuto, invece, a ricercare o raccogliere altri dati che, seppure originariamente trattati, non siano nella propria disponibilità e non siano oggetto in alcuna forma di un attuale trattamento.

In particolare, in uno dei casi sottoposti all'esame del Garante (*Provv.* 21 dicembre 2005 [doc. *web* n. 1217532]), concernente il riscontro a varie istanze di accesso rivolte da una dipendente all'azienda ospedaliera di appartenenza, si è evidenziato che tale riscontro non può avere ad oggetto i dati relativi a terzi, anche di natura sensibile, contenuti nelle richieste di diagnosi e cura sottoscritte dalla ricorrente. Il riscontro può riguardare legittimamente i dati relativi all'interessata consistenti nel suo nome e cognome, nei casi in cui nelle medesime richieste figuri (o vi sia associata) una sottoscrizione intelligibile di quest'ultima, ma non obbliga comunque il titolare del trattamento a fornire copia di tutti i supporti cartacei che li contengano, né tanto meno ad indicare quali e quanti siano tali documenti nel caso in cui i dati siano estrapolati e comunicati nei modi previsti dal Codice (art. 10, comma 4).

Valutazione dei dirigenti

In risposta ad un quesito presentato da un dirigente statale, cui l'amministrazione di appartenenza aveva negato l'accesso ai documenti concernenti la valutazione dei propri colleghi, effettuata ai fini dell'assegnazione del premio di risultato, è stato ribadito che le informazioni di tipo valutativo, ivi compresi i giudizi, le valutazioni e gli altri elementi sui quali si basi eventualmente il giudizio sintetico espresso in occasione della valutazione dei dirigenti, sono dati personali e, in quanto tali, soggetti alla disciplina del Codice (*v.* in particolare, l'art. 8, comma 4, del Codice). Per questo motivo, tali informazioni, ove detenute da una pubblica amministrazione, possono essere rese conoscibili a soggetti privati diversi dalla persona cui si riferiscono, soltanto in base ad una previsione legislativa o regolamentare (art. 19, comma 3, del Codice).

Le disposizioni sull'accesso ai documenti amministrativi, applicabili anche al procedimento di valutazione dei dirigenti per espressa indicazione dell'art. 1, comma 5, d.lg. 30 luglio 1999, n. 286, rappresentano peraltro un'idonea base normativa per la comunicazione a terzi dei dati personali, eventualmente contenuti negli atti cui è rivolta l'istanza di accesso. In questo caso, spetta all'amministrazione destinataria del-

l'istanza di accesso verificare, di volta in volta, l'accoglibilità, o meno, di singole istanze di accesso alla documentazione valutativa, appurando i presupposti legittimanti l'accesso del richiedente, nonché le ragioni in base alle quali tali documenti debbano essere sottratti alla sua conoscibilità (*Nota* 7 febbraio 2005).

Tutela della dignità e riservatezza dei dipendenti

A seguito di una segnalazione il Garante è intervenuto a tutela della dignità e della riservatezza di una lavoratrice i cui dati personali, riguardanti la sua inidoneità al servizio dichiarata da "una commissione medica", erano stati riportati su alcuni atti interni concernenti lo svolgimento di una riunione svoltasi tra alcuni dipendenti, e successivamente affissi all'albo dell'ufficio.

Al riguardo, è stato accertato che le informazioni riportate nel materiale affisso, pur non fornendo alcuna specifica indicazione sui motivi di salute ritenuti all'origine dell'inidoneità della lavoratrice, facevano indirettamente riferimento alle condizioni di salute dell'interessata ed erano perciò da ritenersi "sensibili", in quanto il riscontro dell'inidoneità al servizio era derivato dal pronunciamento di una commissione medica, del quale negli atti affissi si faceva espressa menzione.

L'Autorità ha inoltre rilevato che, nel caso di specie, la diffusione non poteva ritenersi lecita, ponendosi in contrasto con i principi di proporzionalità, indispensabilità, pertinenza e non eccedenza, nonché con le cautele di cui all'art. 22 del Codice. In conformità a tali principi, l'esigenza di rendere noti ai colleghi non presenti alla riunione gli argomenti affrontati avrebbe potuto essere, infatti, utilmente soddisfatta mediante altre modalità di messa a disposizione delle informazioni, maggiormente rispettose della dignità e della riservatezza dell'interessata, come, ad esempio, la consegna in plico chiuso ai colleghi dei documenti affissi all'albo (*Nota* 23 novembre 2005).

Personale delle forze armate e di polizia

Con riferimento al trattamento di dati personali nell'ambito della gestione del personale delle forze armate e di polizia, l'Autorità ha esaminato due casi di opposizione al trattamento posto in essere dalla Guardia di finanza ai fini dell'accertamento della responsabilità disciplinare del personale.

In un primo caso, il Garante ha rilevato che, nell'ambito di tali attività, può essere lecitamente comunicata, ai superiori di un finanziere, la richiesta di archiviazione avanzata da un pubblico ministero in ordine ad una denuncia presentata dall'interessato nei confronti di altri componenti del Corpo, al fine di verificare eventuali violazioni delle disposizioni del regolamento di disciplina militare (in particolare, dell'art. 52, comma 5, lett. *b)*, d.P.R. n. 545/1986, il quale prevede che il militare sia tenuto a comunicare al proprio comando gli "*eventi in cui fosse rimasto coinvolto e che possono avere riflessi sul servizio*") ed avviare, se necessario, il procedimento di contestazione di una infrazione disciplinare (*Provv.* 28 settembre 2005 [doc. *web* n. 1180099]).

In un altro caso è stata ritenuta lecita la comunicazione alle superiori gerarchie del Corpo di vicende riguardanti l'interessato, che lo avevano indotto ad inoltrare una comunicazione di notizia di reato alle competenti autorità giudiziarie militari. Tali informazioni facevano infatti riferimento ad accadimenti di interesse, sia sotto il profilo amministrativo, sia, eventualmente, sotto quello disciplinare, verificatisi nella caserma presso cui l'interessato prestava servizio; non costituivano, nella specie, una violazione delle disposizioni sul segreto nelle indagini preliminari (art. 329 c.p.p.), dal momento che non contenevano alcun riferimento ad atti di indagine (*Provv.* 3 novembre 2005 [doc. *web* n. 1198494]).

Immigrazione

Per quanto riguarda l'attività connessa con l'ingresso e la regolarizzazione dei cittadini extracomunitari, il Garante è intervenuto in riferimento alla predisposizione della modulistica utilizzata per le esigenze dello Sportello unico per l'immigrazione. Il Ministero dell'interno ha chiesto infatti il parere all'Autorità in merito ad un

decreto relativo alla modulistica necessaria al rilascio di provvedimenti di nulla osta in materia di assunzione di lavoratori stranieri o di ricongiungimento familiare.

Il Garante ha evidenziato la necessità di perfezionare l'informativa da rendere all'interessato e di individuare correttamente il titolare di trattamento; è stata inoltre richiamata l'esigenza di rispettare i principi di necessità, pertinenza e non eccedenza nel trattamento dei dati raccolti con la modulistica rispetto alle finalità perseguite, con particolare riguardo ai dati idonei a rivelare lo stato di salute del datore di lavoro in caso di lavoro domestico per assistenza (*Provv.* 25 maggio 2005 [doc. *web* n. 1131847]).

12.2. *Previdenza*

Trasmissione telematica dei certificati di malattia all'Inps

La legge finanziaria 2005 ha stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante debba trasmettere all'Inps, per via telematica, il certificato di diagnosi sull'inizio e sulla durata presunta della malattia. La definizione delle specifiche tecniche e delle modalità procedurali è demandata ad un apposito decreto interministeriale di iniziativa del Ministero del lavoro e della previdenza sociale (art. 1, comma 149, l. n. 311/2004). Con il più volte richiamato *provvedimento* del 25 maggio 2005 il Garante –che dovrà essere comunque chiamato ad esprimere un parere su tale decreto– ha richiesto preventivamente che vengano individuate in tale sede soluzioni efficaci e rispettose dei principi in materia di protezione dei dati personali.

Accesso dei patronati a banche dati previdenziali

Su specifica richiesta dell'Inps, l'Autorità ha inoltre esaminato uno schema di protocollo volto a consentire ai patronati la consultazione delle posizioni relative agli assicurati contenute nelle banche dati dell'istituto previdenziale e, in particolare, nel Casellario centrale delle posizioni previdenziali (l. 23 agosto 2004, n. 243; d.m. 4 febbraio 2005, in *G.U.* 29 marzo 2005, n. 72).

Le modalità previste nello schema di protocollo sono state ritenute, allo stato, conformi alle disposizioni in materia di protezione dei dati personali, in attesa che vengano stabilite con decreto del Ministro del lavoro e delle politiche sociali le linee-guida per apposite convenzioni da stipularsi tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni, e ferme restando le possibili indicazioni che il Garante potrà impartire nel parere previsto sul medesimo decreto. Il protocollo prevede infatti che i patronati possano accedere alle banche dati dell'istituto, ma nell'ambito del mandato conferito dall'interessato e sulla base del consenso manifestato in relazione a tipi di dati individuati specificamente (art. 116 del Codice).

La circostanza che le disposizioni sul Casellario centrale delle posizioni previdenziali non menzionino espressamente i patronati tra i soggetti legittimati ad accedervi non è stata, peraltro, ritenuta ostativa della possibilità di consentire ai patronati stessi la consultazione delle informazioni contenute nella banca dati, nella misura in cui ciò avvenga alle condizioni e per le sole finalità previste dall'art. 116 del Codice (*Nota* 8 febbraio 2006).

Informativa rilasciata agli assistiti da istituti di patronato

L'Ufficio del Garante ha fornito altresì la propria collaborazione per l'elaborazione, su iniziativa di un gruppo di rappresentanti di alcuni istituti di patronato e di assistenza sociale, di un modello di informativa da fornire agli interessati che decidano di farsi assistere e rappresentare da tali enti nello svolgimento di pratiche relative a prestazioni in materia di previdenza, assistenza sociale e sanitaria.

Prestazioni sociali agevolate

A seguito della segnalazione inoltrata da un'associazione, l'Ufficio si è pronunciato circa il trattamento di dati personali effettuato da un istituto previdenziale, ai fini del riconoscimento di prestazioni sociali agevolate nei confronti di soggetti con

12

handicap permanente grave e di soggetti ultra-sessantacinquenni non autosufficienti. La normativa di settore demanda ad un apposito decreto del Presidente del Consiglio dei ministri l'individuazione delle informazioni da dichiarare, in modo da evidenziare la situazione economica del solo assistito (art. 3, comma 2-*ter*, d.lg. n. 109/1998). Pur nella persistente mancanza di tale decreto attuativo, su cui l'Autorità dovrà essere chiamata ad esprimere il proprio parere, si è ritenuto che il rispetto dei principi di indispensabilità, pertinenza e non eccedenza dei dati raccolti rispetto alle finalità perseguite, imponga all'istituto di raccogliere soltanto le informazioni personali relative alla situazione economica degli interessati, e non anche quelle relative ai componenti del nucleo familiare di appartenenza (*Nota* 24 marzo 2006).

Incaricati del trattamento di dati previdenziali

L'Autorità è intervenuta in un caso riguardante il trattamento di dati personali relativi all'estratto della posizione contributiva dell'interessato, acquisiti presso gli archivi di un istituto previdenziale e successivamente utilizzati dal coniuge –dipendente di una sede provinciale del medesimo istituto– nel giudizio di separazione legale. In seguito alle lamentele dell'interessato, l'istituto aveva, nel frattempo, oscurato la sua posizione contributiva in modo da evitare ulteriori accessi non autorizzati.

L'Ufficio ha rilevato che spetta all'istituto impartire adeguate istruzioni ai propri dipendenti in merito all'accesso e all'utilizzo delle informazioni da essi conoscibili ed assicurare la corretta applicazione della disciplina sulla protezione e sulla sicurezza dei dati, anche in riferimento a possibili trattamenti illeciti o non conformi alle finalità della raccolta, ascrivibili anche alla condotta di singoli dipendenti (artt. 31-36 del Codice). La sede interessata è stata pertanto invitata a far conoscere le iniziative e gli accorgimenti assunti per rendere il trattamento conforme alle disposizioni sulla sicurezza e per ripristinare, nei casi e nei modi consentiti, l'accesso dell'interessato ai dati personali relativi alla sua posizione contributiva.

Quanto all'utilizzo dei dati dell'interessato nel giudizio di separazione legale è stato precisato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nei procedimenti giudiziari basati sul trattamento, e quindi anche sulla eventuale raccolta illecita di dati personali, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 11, comma 2, e 160, comma 6, del Codice) (*Nota* 11 novembre 2005).

13 Videosorveglianza

Anche nel corso del 2005, il Garante ha avuto occasione di occuparsi delle tematiche relative all'impianto ed all'utilizzo di sistemi di videosorveglianza.

Abitazioni private

Con riferimento all'installazione di impianti di videosorveglianza presso abitazioni, è stato nuovamente ribadito in una decisione adottata su ricorso che le disposizioni del Codice non risultano applicabili al trattamento di dati effettuato per fini personali, pur restando ferma l'osservanza degli obblighi in materia di sicurezza e di risarcimento dell'eventuale danno, nonché la facoltà dei soggetti che ritengono di aver subito un danno per effetto del trattamento dei dati di far valere i propri diritti in ordine alla liceità e correttezza della raccolta e dell'utilizzazione delle immagini (*Provv.* 27 ottobre 2005 [doc. *web* n. 1193121]).

13.1. *Videosorveglianza in ambito pubblico*

In relazione all'ambito pubblicistico molteplici segnalazioni e quesiti hanno evidenziato come, nonostante i ripetuti interventi del Garante, a due anni dall'adozione del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482], lo stato di attuazione della disciplina in materia di videosorveglianza non risulti ancora del tutto soddisfacente, essendo emerse situazioni diffuse caratterizzate dall'omessa o inidonea applicazione delle regole fissate. Anche per questo, sono risultate numerose le occasioni per ribadire le indicazioni per un corretto utilizzo di telecamere da parte di soggetti pubblici in specifici settori.

Scuole

Con riferimento all'installazione di sistemi di videosorveglianza presso istituti scolastici l'Autorità ha riaffermato la vigenza delle prescrizioni fornite con il provvedimento generale. In ordine all'attivazione di telecamere all'interno dell'edificio di un istituto anche durante l'orario delle lezioni, è stata ad esempio rappresentata la necessità di limitarla ai casi di stretta indispensabilità, come ad esempio, a causa di ripetuti atti vandalici e comunque al di fuori dell'orario scolastico, quando gli edifici sono chiusi, anche in ragione del fatto che possono essere altrimenti raccolti indebitamente dati riguardanti minori di età e di lavoratori (*Nota* 26 aprile 2005). Nella predetta circostanza l'Ufficio ha invitato l'istituto a produrre ogni documento utile a sostegno delle iniziative assunte al fine di rendere il trattamento dei dati effettuato conforme al quadro di garanzie delineato nel provvedimento generale, ricevendo un riscontro sul quale sono in corso ulteriori accertamenti.

Telecamere mobili

In un diverso ambito il Garante ha fornito riscontro ad una richiesta pervenuta in merito all'utilizzo, da parte di alcuni comuni, di telecamere mobili installate su automezzi e posizionate temporaneamente in siti prestabiliti individuati di volta in volta in base a contingenti esigenze di sicurezza. In proposito, l'Autorità ha ribadito il necessario rispetto del principio di proporzionalità tra i mezzi impiegati e i fini perseguiti; in particolare, secondo tale principio, impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente ritenute insufficienti o inattuabili. Tale valutazione deve essere, poi, effettuata specificamente anche in riferimento alla dislocazione, all'angolo visuale e alle tipologie –fisse o mobili– delle apparecchiature installate. Anche per le telecamere di tipo mobile

13

Presupposti per la videosorveglianza da parte dei comuni

restano valide le indicazioni specifiche relative all'installazione di sistemi di videosorveglianza presso, ad esempio, luoghi di culto o di sepoltura o per il controllo di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose (*Nota* 8 novembre 2005).

In diverse occasioni sono stati forniti altri chiarimenti circa la possibilità, per i comuni, di attivare sistemi di videosorveglianza. In particolare è stato evidenziato che l'utilizzo di sistemi di videosorveglianza può essere giustificato solo ed esclusivamente dallo svolgimento di funzioni istituzionali che la stessa amministrazione è tenuta ad individuare ed esplicitare con esattezza e di cui essa sia effettivamente titolare in base all'ordinamento di riferimento (*Note* 16 e 22 febbraio 2005, 7 e 22 aprile 2005, 21 ottobre 2005 e 12 dicembre 2005).

È stata richiamata inoltre, in proposito, l'opportuna attenzione sul necessario rispetto di tutte le prescrizioni contenute nel *provvedimento* generale del 29 aprile 2004, ivi comprese la designazione dei responsabili o incaricati del trattamento, la predisposizione dell'informativa da rendere agli interessati (utilizzando eventualmente il modello semplificato messo a disposizione dal Garante in allegato al citato provvedimento) e l'adozione delle misure minime di sicurezza.

Discariche abusive e orario di deposito dei rifiuti urbani

Sono state nuovamente confermate le indicazioni già fornite a proposito dell'utilizzo di sistemi di videosorveglianza presso aree abusivamente impiegate come discariche di materiali, ricordando che tale utilizzo è lecito solo qualora risultino inefficaci o inattuabili altre misure; per converso, non risulta lecito un controllo video al solo scopo di accertare infrazioni amministrative rispetto a disposizioni concernenti le modalità e l'orario di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori (*Note* 29 dicembre 2004 e 22 febbraio 2005). In un caso, a seguito della segnalazione pervenuta da un'associazione di risparmiatori e consumatori, l'Ufficio del Garante ha invitato a conformarsi alle citate prescrizioni un comune che intendeva "monitorare" le operazioni di smaltimento dei rifiuti per verificare il rispetto delle disposizioni sulla raccolta differenziata. L'ente locale ha comunicato di aver disattivato il sistema di registrazione e di aver cancellato tutte le immagini registrate (*cfr. Newsletter* 21-27 febbraio 2005).

Accesso ai centri storici e Ztl

L'Autorità è stata nuovamente interpellata in riferimento all'installazione di sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato. Si è confermato che i comuni devono richiedere una specifica autorizzazione amministrativa e limitare la rilevazione delle immagini ai soli casi di infrazione (art. 3 d.P.R. 22 giugno 1999, n. 250). I dati così trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e per definire il relativo contenzioso; alle informazioni si può accedere solo a fini di polizia giudiziaria o di indagine penale (*Note* 22 febbraio 2005).

Strutture sanitarie

Rigorose e specifiche cautele sono state richiamate anche in relazione all'attivazione di impianti di videosorveglianza in alcune aree di un *campus* ospedaliero e presso gli ingressi di una sede di un'azienda sanitaria (*Note* 22 febbraio 2005 e 12 aprile 2005). In particolare, nel rappresentare che l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria per finalità di sicurezza può evidenziare anche profili inerenti alle condizioni di salute dei pazienti, è stato confermato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (*ad es.*, unità di rianimazione) devono essere limitati a casi di stretta indispensabilità, circoscrivendo le riprese solo a determinati locali e a precise fasce orarie e adottando tutti gli accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate. Nelle stesse occasioni è stato fatto nuovamente presente che possono accedere alle immagini solo i soggetti specificamente autorizzati (*ad es.*, personale

medico ed infermieristico), non potendo le stesse essere visionate da estranei (*ad es.*, visitatori), e che le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice).

Luoghi di lavoro

Per quanto riguarda l'installazione di impianti video nei luoghi di lavoro è stato ricordato ad una prefettura e ad una direzione provinciale di un istituto previdenziale, come già rilevato in precedenti provvedimenti dell'Autorità, che detta installazione potrebbe coinvolgere anche i lavoratori dipendenti e configurare pertanto un controllo a distanza nei confronti dei lavoratori. A tale proposito è stata nuovamente richiamata l'attenzione sulle garanzie previste per i rapporti di lavoro anche quando gli impianti sono utilizzati per esigenze organizzative e dei processi produttivi, ovvero sono richiesti per la sicurezza del lavoro, con particolare riferimento al principio contenuto nell'art. 4 dello Statuto dei lavoratori che sancisce il divieto di controllo a distanza dell'attività dei lavoratori (*Note* 8 e 22 febbraio 2005). Non è stata invece rinvenuta lesiva del citato principio la condotta di un ente di ricerca che aveva installato alcune telecamere a tutela della sede di una segreteria ove veniva esplicata una delicata funzione di sicurezza (*Nota* 2 febbraio 2006).

Impianti sportivi

L'Autorità è stata chiamata a pronunciarsi anche a proposito dell'attivazione di sistemi di videosorveglianza presso impianti sportivi di capienza superiore alle diecimila unità, in occasione di competizioni calcistiche.

In particolare, il Garante ha espresso parere riguardo a due schemi di decreto, predisposti dal Ministero dell'interno in attuazione di un decreto-legge (n. 28/2003) che prevede, tra le misure contro la violenza negli stadi, oltre al rilascio di biglietti numerati, anche l'introduzione di telecamere fisse. Al riguardo, l'Autorità ha stabilito che il controllo svolto mediante videosorveglianza, basandosi su un idoneo fondamento normativo, risulta rispettoso del principio di liceità (art. 11, comma 1, lett. *a)*, del Codice) ed è altresì giustificato alla luce del principio di necessità e proporzionalità nel trattamento dei dati, anche in ragione dei reiterati disordini e degli episodi di violenza verificatisi. Sono state poi considerate, in termini generali, proporzionate, alcune disposizioni in materia di conservazione dei dati, di modalità di ripresa e di tipologia di informazioni rilevabili, risultando trattati dati pertinenti e non eccedenti rispetto alle finalità di tutela dell'ordine pubblico e della sicurezza e di accertamento di reati.

Il Garante ha chiesto di limitare l'ambito applicativo ai soli impianti sportivi di capienza superiore alle diecimila unità e ad eventi in occasione di competizioni calcistiche, derivando questi limiti direttamente dalla norma di legge, e di espungere riferimenti ad altri ambiti applicativi non previsti da tale norma (*Parere* 4 maggio 2005 [doc. *web* n. 1120732]).

Accanto a diverse altre indicazioni (deliminazione dell'ambito geografico di alcune riprese alle "immediate vicinanze degli impianti"; registrazioni audio del solo evento calcistico in generale; individuazione del soggetto che dovrebbe prescrivere misure di sicurezza; modalità di previsione dell'obbligo di porre dati e supporti a disposizione dell'autorità o della polizia giudiziaria), il Garante ha affrontato analiticamente la questione della previsione di biglietti nominativi di accesso agli stadi, aggiuntiva rispetto a quella dei biglietti numerati.

L'Autorità ha richiamato l'attenzione sulle misure di controllo di altro tipo introdotte in altri Paesi constatando che il decreto-legge introduce solo l'obbligo di numerare i biglietti e sollecitando quindi una verifica circa la possibilità di introdurre questo ulteriore vincolo con un provvedimento amministrativo. Rilevato poi che la nominatività dei biglietti comporta la creazione di grandi banche dati relative a diverse centinaia di migliaia di interessati, il Garante ha rilevato che a sostegno della richiesta di parere non erano stati allegati specifici elementi che potessero per-

mettergli di ritenere allo stato proporzionata "*una misura delicata di cui, a fronte degli innumerevoli dati personali che dovrebbero essere trattati, dovrà essere valutata attentamente la proporzione e l'effettiva utilità in rapporto alle finalità perseguite e alle più frequenti modalità con cui si svolgono incidenti negli stadi. Ciò, tenendo anche conto che potrebbero essere attivati altri controlli di sicurezza per identificare tifosi violenti ed escluderli dagli stadi…valutando infine la circostanza che i biglietti nominativi non risultano utilizzati diffusamente in altri Paesi dell'Unione europea (a parte i titoli di abbonamento, rilasciati per altre finalità*".

Sulla videosorveglianza in generale, allo scopo di verificare la conformità alle indicazioni contenute nel provvedimento generale sulla videosorveglianza, è stata sviluppata un'intensa attività ispettiva che ha evidenziato in più occasioni un rispetto non ancora rigoroso della disciplina, con particolare riferimento alla liceità dei sistemi installati, all'idoneità della necessaria informativa all'utenza, alle modalità di raccolta dei dati e ai tempi di conservazione delle immagini raccolte.

13.1.1. *Richieste di verifica preliminare*

In casi frequenti, il riscontro alle richieste di chiarimenti in materia di videosorveglianza ha fornito al Garante l'occasione per precisare che l'installazione di sistemi di videosorveglianza non deve essere generalmente sottoposta all'esame preventivo dell'Autorità e che non può per converso desumersi, dal mancato riscontro, alcuna approvazione implicita dalla trasmissione al Garante di comunicazioni o progetti relativi alla intenzione di installare sistemi di videosorveglianza. Non è del resto stabilito alcun termine decorso il quale i progetti sottoposti alla verifica dell'Autorità possano ritenersi dalla stessa autorizzati, non applicandosi neanche il principio del silenzio-assenso; deve ritenersi, invece, che il *provvedimento* 29 aprile 2004 abbia individuato espressamente le specifiche ipotesi in cui i titolari del trattamento sono tenuti a sottoporre alla verifica preliminare i sistemi di videosorveglianza che si intendono attivare.

14 Altre iniziative nel settore pubblico

14.1. *Utilizzo di dati biometrici*

In ambito pubblico sono pervenute numerose segnalazioni, nonché specifiche richieste di parere da parte di comuni, in merito all'utilizzo di sistemi di rilevazione automatica delle presenze mediante il riconoscimento delle impronte digitali. L'Autorità ha avviato nuove istruttorie in merito alla liceità dell'utilizzo di tali sistemi per il controllo dell'accesso al luogo di lavoro da parte dei dipendenti.

14.2. *Ulteriori iniziative dell'Ufficio*

Progetto *"Dove siamo nel mondo"*

L'Unità di crisi del Ministero degli affari esteri ha sottoposto all'esame del Garante un progetto denominato "*Dove siamo nel mondo*" per una valutazione preliminare in ordine alla sua compatibilità con la normativa in materia di protezione dei dati personali. Il progetto, nell'ambito dell'ottimizzazione della gestione di situazioni di crisi internazionali legate a calamità naturali, attentati terroristici ed altre emergenze, è volto a consentire ai cittadini italiani di segnalare al Ministero degli esteri, su base volontaria, i propri recapiti ed itinerari, al fine di facilitare la localizzazione, l'invio di eventuali avvisi o l'intervento di soccorso in caso di emergenze.

L'Ufficio del Garante ha indicato al Ministero le necessarie cautele da adottare nella realizzazione del progetto, con particolare riferimento alle tipologie di dati richiesti, alla loro gestione e conservazione, nonché all'informativa da fornire all'interessato e all'eventuale coinvolgimento di terzi.

La versione definitiva del progetto prevede la creazione di un apposito sito Internet attraverso il quale i cittadini, previa idonea informativa, possono inserire su base volontaria le proprie generalità ed informazioni sul viaggio (*ad es.*, paese di destinazione, date di partenza e di rientro, località di permanenza, dettagli dell'itinerario e recapiti); i dati registrati saranno automaticamente cancellati trascorse quarantotto ore dalla data di rientro. Il titolare del trattamento è il Ministero degli esteri e la banca dati è gestita unicamente dall'Unità di crisi. I dati raccolti sono utilizzati esclusivamente per lo studio e la realizzazione di piani di intervento per la sicurezza degli italiani all'estero in situazioni di crisi e potranno essere comunicati a determinati soggetti terzi al solo fine di assicurare assistenza in caso di emergenza.

15 Reti di comunicazione elettronica

15.1. *Conservazione dei dati di traffico*

Successivamente alle già ricordate modifiche apportate all'art. 132 del Codice dall'art. 3 del d.l. 24 dicembre 2003, n. 354, convertito, con modificazioni, dalla l. 26 febbraio 2004, n. 45 (*v. Relazione* 2004, p. 97), si è assistito, nel 2005, ad un nuovo, significativo intervento normativo, che ha ulteriormente innovato la disciplina della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati (sul quale *v.* par. 1.1).

In tale contesto, il Garante, che aveva già avviato, conformemente alla previsione dell'art. 132, comma 5, del Codice, i lavori necessari per individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le richiamate finalità di accertamento e repressione dei reati, ha esteso al traffico telematico l'ambito di verifica preliminare dei sistemi attualmente utilizzati dagli operatori, in vista della programmata predisposizione del provvedimento previsto dalla predetta disposizione.

15.2. *I nuovi elenchi telefonici*

Nella *Relazione* 2004 (p. 99) si era dato conto del provvedimento di carattere generale con il quale il Garante, ai sensi dell'art. 129, comma 2, del Codice, nonché in ragione delle modifiche introdotte nella disciplina degli elenchi telefonici, aveva individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali relativi ad abbonati (e utilizzatori di schede prepagate) nei nuovi elenchi telefonici (*cfr. Provv.* 15 luglio 2004 [doc. *web* n. 1032381]).

Successivamente all'adozione del provvedimento il Garante ha fornito agli operatori prescrizioni integrative con riferimento ai moduli per l'informativa e la raccolta dei consensi predisposti dagli operatori, ed ha avviato altresì la campagna informativa prevista nel provvedimento stesso. L'Autorità ha, inoltre, avviato direttamente una prima campagna di informazione con un apposito *depliant* messo a disposizione degli operatori e attraverso una conferenza stampa tenutasi presso la sede dell'Autorità il 26 gennaio 2005.

Nel 2005 il Garante ha monitorato con attenzione, anche tramite varie richieste di informazioni agli operatori, il rispetto delle scadenze per l'attuazione della nuova disciplina indicate nel ricordato *provvedimento* del 15 luglio 2004 (*cfr.* l'allegato III del provvedimento).

L'Ufficio, anche in risposta ad alcuni quesiti pervenuti in tema di utilizzabilità dei dati presenti nei nuovi elenchi telefonici da parte di soggetti operanti per finalità non di lucro, ha specificato che la nuova disciplina degli elenchi opera a prescindere dall'eventuale fine di profitto perseguito. Pertanto, ogni uso dei dati presenti nei nuovi elenchi diverso dalla comunicazione interpersonale, quali ad esempio le attività di carattere pubblicitario e promozionale, resta possibile solo con il consenso preventivo degli interessati. Il Garante ha altresì evidenziato come gli enti che perseguono finalità di carattere socio-assistenziale o di interesse collettivo o diffuso continuino, in ogni caso, a disporre di altre modalità per il reperimento dei dati perso-

nali dei potenziali sostenitori, in particolare tramite l'accesso alle liste elettorali (*cfr.* art. 51, d.P.R. n. 223/1967, come modificato dall'art. 177 del Codice).

È stato inoltre rilevato che la nuova disciplina può non operare con riguardo ai dati personali estratti precedentemente dai vecchi elenchi e già effettivamente (e non elusivamente) registrati sempre in precedenza in una banca dati, eventualmente inseriti insieme ad altre informazioni tratte da ulteriori fonti. L'utilizzazione di questi dati è lecita solo se, al momento della loro registrazione, è stata fornita un'idonea informativa agli interessati, instaurando così con gli stessi un "rapporto" nell'ambito del quale il titolare del trattamento è rimasto comunque obbligato a cancellare i dati di chi lo richieda. Se, però, la predetta informativa non è stata resa tempestivamente a norma di legge, il trattamento è stato ed è rimasto illecito; il titolare non può in alcun modo utilizzare i dati e deve necessariamente cancellarli per non incorrere in serie sanzioni. Per quanto concerne il necessario aggiornamento delle informazioni contenute nelle menzionate banche dati, è stato ribadito che lo stesso potrà avvenire soltanto sulla base delle nuove regole sull'uso degli elenchi telefonici.

15.3. *Elenchi telefonici* cd. *"categorici"*

Nel periodo di riferimento, il Garante ha valutato l'opportunità di intervenire in riferimento alla problematica degli elenchi telefonici organizzati per categorie merceologiche/professionali (*cd.* elenchi "categorici"). Tenendo conto del carattere commerciale e promozionale dei menzionati elenchi "categorici", che contengono informazioni relative allo svolgimento delle attività economiche ed equiparate dei soggetti interessati (in particolare aziende, professionisti, esercizi commerciali ed enti), nonché delle specifiche finalità degli stessi non riconducibili esclusivamente alla *"mera ricerca dell'abbonato per comunicazioni interpersonali"*, il Garante ha individuato a favore degli editori di tali elenchi un particolare regime di semplificazione (*Provv.* 14 luglio 2005 [doc. *web* n. 1151640]).

Si è infatti chiarito che, per la formazione degli elenchi in questione, gli editori possono avvalersi della previsione del Codice che permette di prescindere dal consenso degli interessati quando il trattamento riguarda appunto "dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d)*, del Codice). Devono essere comunque rispettati gli altri obblighi e diritti in materia di protezione dei dati personali: in particolare, deve essere garantita la completezza dei nominativi degli interessati riportati nelle diverse tipologie di elenchi pubblicati e, nel caso in cui i dati siano attinti dal nuovo "*database* unico", di cui all'allegato II del predetto *provvedimento* del 15 luglio 2004, non possono essere pubblicati gli estremi identificativi di coloro che abbiano eventualmente manifestato la volontà di non comparire negli elenchi telefonici "alfabetici".

L'Autorità, infine, ai sensi dell'art. 13, commi 4 e 5, lett. *c)*, del Codice, ha autorizzato i suddetti titolari del trattamento a fornire a professionisti, esercenti, aziende ecc., che compariranno nell'elenco, un'informativa semplificata tramite la pubblicazione di appositi avvisi su quotidiani, nonché nella parte iniziale dell'elenco "categorico" cartaceo e di quello pubblicato *on-line*.

15.4. Spamming

Anche nel corso del 2005 si è mantenuta elevata l'attenzione dell'Autorità rispetto alla pratica dello *spamming* (invio di messaggi promozionali indesiderati

all'indirizzo di posta elettronica dei destinatari). Sono state, fra l'altro, intensificate le attività di controllo e verifica delle attività svolte da diversi operatori che, direttamente o per mezzo di soggetti specializzati, svolgono campagne pubblicitarie e di *direct marketing* utilizzando tale nuovo mezzo di comunicazione. Risulta, poi, in fase conclusiva l'istruttoria già avviata nei confronti di due importanti società operanti *on-line*, che utilizzano migliaia di indirizzi di posta elettronica per finalità promozionali e commerciali di prodotti e servizi propri e di altre aziende.

Particolare preoccupazione ha destato, tra l'altro, l'incremento delle segnalazioni che lamentano l'invio di *e-mail* riconducibili al fenomeno denominato "*phishing*", consistente nell'uso di messaggi di posta elettronica e nella creazione di pagine *web* progettate per simulare comunicazioni ufficiali da parte soprattutto di istituti di credito, con la finalità di raggirare gli utenti Internet per carpire dati personali o acquisire fraudolentemente informazioni riguardanti la carta di credito o il conto corrente bancario.

In ambito internazionale, nel periodo considerato, l'Autorità ha partecipato attivamente ai lavori del Cnsa (*Contact Network of Spam Authorities*) che si tengono presso la Commissione europea-Direzione generale società dell'informazione e media. Nei vari incontri, cui partecipano le istituzioni di settore di tutti i Paesi membri, si è proceduto a valutare vari strumenti di intervento per intensificare la lotta allo *spam*. È in corso la predisposizione di un documento comune, denominato *London Action Plan*, che definirà le procedure utili a facilitare le indagini sullo *spam* anche attraverso la semplificazione delle modalità di contatto tra le istituzioni partecipanti.

Tra le attività di carattere internazionale finalizzate a contrastare il fenomeno dello *spam* va ricordata anche la *task force* istituita presso l'Ocse, ai cui lavori ha partecipato anche l'Autorità, e che ha redatto nel 2005 una bozza di raccomandazione sulla "cooperazione transfrontaliera nel rafforzamento delle leggi contro lo *spam*" (sul punto, *v.* par. 22.3).

15.5. *Videochiamate*

I nuovi servizi telefonici disponibili attraverso l'impiego di telefoni mobili definiti "di terza generazione", tramite diverse tecnologie di rete, quali *Gprs*, *Edge* o *Umts*, sono stati già oggetto di attenzione da parte dell'Autorità (*cfr. Relazione* 2004, pp. 100-101).

Rispetto al semplice utilizzo dei messaggi del tipo *Sms* e *Mms*, in ordine ai quali il Garante si è più volte pronunciato in passato, i "videotelefono" offrono nuove funzionalità. Questi apparecchi sono dotati di videocamere di dimensioni molto ridotte, orientabili in vario modo, e dispongono di diverse funzioni mediante le quali si possono agevolmente raccogliere, comunicare e diffondere immagini e suoni in tempo reale. Tali applicazioni, utili nell'ordinaria vita di relazione interpersonale, possono essere tuttavia utilizzate in modo da violare, anche involontariamente, i diritti delle persone interessate dalla comunicazione, come pure di terzi inconsapevoli della ripresa.

In ragione dei potenziali pericoli insiti nell'utilizzo di tali nuovi strumenti di telefonia, il Garante, all'esito di una consultazione pubblica attivata al fine di acquisire elementi di valutazione, ha individuato le modalità da osservare per un corretto utilizzo dei medesimi strumenti con riferimento al trattamento dei dati (*Provv.* 20 gennaio 2005 [doc. *web* n. 1089812]). In particolare, nell'evidenziare la generale liceità del loro utilizzo per fini esclusivamente personali, l'Autorità ha sottolineato che il Codice –ferme restando altre norme dell'ordinamento– non si applica se le

immagini rimangono nella disponibilità privata di chi ha effettuato le riprese o circolano solo tra un numero ristretto di persone. Si è indicata comunque la necessità che, anche in questi casi, il soggetto che utilizza l'apparecchio rispetti i diritti dei terzi anche in tema di diritto all'immagine eal ritratto, nonché gli obblighi previsti in materia di sicurezza dei dati, tenendo conto della possibilità di essere chiamati a risarcire eventuali danni anche morali cagionati a terzi.

È stata, poi, sottolineata l'illiceità di un'eventuale comunicazione sistematica attraverso il videotelefono o di una diffusione anche via Internet delle immagini, effettuata senza richiedere, quando è necessario, il consenso preventivo, libero e informato (manifestato per iscritto nel caso siano trattati dati sensibili). L'informativa ed il consenso possono riguardare in tal caso non solo i soggetti che si intende ritrarre direttamente, ma anche eventuali terzi, identificati o identificabili, eventualmente ripresi anch'essi nelle immagini.

Il Garante ha richiamato altresì l'attenzione sull'esigenza di verificare se, in determinati uffici pubblici, luoghi pubblici e privati o aperti la pubblico, l'uso dei videotelefoni sia eventualmente inibito: limiti e cautele (introdotti in alcuni Paesi anche con norme di legge) possono essere infatti prescritti legittimamente da soggetti pubblici e privati e, se non rispettati, possono rendere il trattamento dei dati illecito o non corretto. Garanzie analoghe sono state richiamate anche rispetto all'uso di immagini all'interno di forum *on-line*.

L'Autorità ha, infine, invitato imprese produttrici di apparecchi o impegnate nella realizzazione di *software* di valutare l'opportunità di dotare i cellulari di nuove funzioni, tra cui anche segnali luminosi, per rendere più evidente che il videotelefono è in funzione, come pure di sistemi per il blocco della trasmissione dell'immagine senza che venga interrotta la conversazione.

15.6. *Chiamate in entrata*

Il trattamento dei dati personali relativi alle comunicazioni telefoniche in entrata pone delicate implicazioni per la riservatezza delle persone cui gli stessi si riferiscono: oltre a riguardare gli abbonati o i titolari di una carta prepagata, le chiamate in entrata possono coinvolgere altri soggetti quali familiari, amici, membri di una comunità e dipendenti. Per questi motivi, relativamente a tali dati, il Codice non consente di regola agli interessati di rivolgere al fornitore di un servizio di comunicazione elettronica le istanze di cui all'art. 7. Solo in via di eccezione, le richieste di esercizio dei diritti possono essere presentate e riscontrate positivamente, qualora si comprovi che la risposta da parte del fornitore è necessaria per evitare "un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397" (art. 8, comma 2, lett. *f)*, del Codice).

In tale contesto generale, il Garante (intervenuto già in passato sull'argomento in occasione dell'esame di ricorsi e segnalazioni) ha ritenuto necessario richiamare l'attenzione degli operatori telefonici sui limiti entro i quali i fornitori dei servizi di comunicazione elettronica accessibili al pubblico possono rispondere positivamente ad una richiesta *ex* art. 7 del Codice, impartendo ad essi alcune prescrizioni con un apposito provvedimento di carattere generale (*Provv.* 3 novembre 2005 [doc. *web* n. 1189488]).

All'interno di quest'ultimo, è stato di nuovo posta in rilievo la disposizione codicistica che prevede che l'abbonato o il titolare di una carta prepagata possa conoscere i dati personali relativi al traffico telefonico in entrata, *Sms* ed *Mms* compresi, solo dimostrando l'indispensabilità dell'acquisizione di tali informazioni allo scopo

di tutelare i propri diritti in sede penale, in quanto la mancata conoscenza delle stesse determinerebbe un danno effettivo e concreto al diritto di difesa. I dati in tal modo conosciuti non possono essere utilizzati per altri scopi: a tal fine, il fornitore deve richiedere il rilascio di una dichiarazione, dall'interessato o dall'avvocato cui sia stato conferito mandato, che attesti la veridicità di quanto prospettato e manifesti l'impegno a non utilizzare i dati per altre finalità. Possono essere peraltro prese in considerazione solo le richieste corredate da una motivazione in cui sia specificata l'intenzione di utilizzare i dati nell'ambito di un procedimento penale, risultando pertanto escluse quelle riguardanti controversie civili e di volontaria giurisdizione.

È stato inoltre individuato in capo al fornitore del servizio l'obbligo di accertare con scrupolo l'identità e la legittimazione del richiedente, nonché quello di fornire un riscontro, seppur negativo, entro quindici giorni dal ricevimento dell'istanza. Non vi è, per converso, necessità di un'autorizzazione dell'autorità giudiziaria per comunicare i dati, né occorre che il richiedente documenti anche il numero di repertorio di un procedimento penale, in ragione del fatto che le indagini difensive possono essere avviate lecitamente anche prima di tale procedimento e per l'eventualità che esso sia instaurato (art. 391-*nonies* c.p.p.).

Sono stati infine specificati i dati che il fornitore potrà comunicare: si tratta del numero del chiamante, della data, dell'ora di inizio e della tipologia della comunicazione e della durata.

15.7. *Intercettazioni*

Nel mese di agosto del 2005, il Garante ha avviato un'indagine nei confronti dei principali gestori di telefonia fissa e mobile riguardo alle modalità con le quali essi adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni.

Gli accertamenti hanno messo in luce che i gestori, pur non venendo a conoscenza dei contenuti delle intercettazioni, raccolgono, selezionano, elaborano ed utilizzano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali questi comunicano. Si tratta di dati personali particolarmente delicati che riguardano l'identità dei soggetti sottoposti ad intercettazione e l'arco temporale di svolgimento dell'intercettazione nonché i dati di traffico telefonico o telematico. In alcuni casi, tali dati sono integrati da informazioni aggiuntive relative alle chiamate in ingresso, ai tentativi di chiamata e alla localizzazione geografica dell'utenza intercettata.

È emerso, inoltre, che gli ulteriori servizi svolti dai fornitori a supporto dell'attività investigativa possono riguardare anche aspetti diversi dalle intercettazioni e comprendere interrogazioni anagrafiche, localizzazione dell'utenza, tracciamento e sospensione dei servizi agli utenti, documentazione del traffico storico. A differenza di quanto avviene con le conversazioni intercettate, i gestori hanno la possibilità di conoscere le informazioni derivanti dall'attivazione di questi servizi, essendo essi stessi ad estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria e ad organizzarli in tabulati. Infine, anche i servizi *Sms* ed *Mms* sono risultati compresi nell'attività di intercettazione.

All'esito dell'istruttoria e sulla base della documentazione pervenuta, l'Autorità ha prescritto ai gestori (*Provv.* 15 dicembre 2005 [doc. *web* n. 1203890]) di adottare alcuni accorgimenti e misure ulteriori nel proteggere i dati allorché adempiano alle menzionate richieste dell'autorità giudiziaria. Le misure riguardano sia gli aspetti organizzativi, sia la sicurezza dei flussi informativi diretti verso l'autorità giudiziaria, sia la protezione dei dati trattati a scopo di giustizia.

I diversi accorgimenti prescritti dal Garante ai fornitori (ai quali è stato assegnato un termine di centottanta giorni per l'adeguamento) riguardano in particolare: l'individuazione più selettiva del ristretto numero di incaricati designati a trattare i dati; la separazione tra i dati di carattere contabile e i dati documentali prodotti nel corso delle attività svolte su richiesta dell'autorità giudiziaria; l'adozione di procedure di autenticazione robuste per l'accesso informatico da parte del personale incaricato ai dati trattati, con il ricorso anche a caratteristiche biometriche; l'adozione di sistemi di comunicazione con l'autorità giudiziaria basati su aggiornati strumenti telematici e tecniche di firma digitale, evitando l'uso di sistemi meno sicuri (*ad es.*, il fax); la protezione dei dati, per il periodo di presenza nelle banche dati dei gestori, con strumenti avanzati di cifratura; la cancellazione immediata dei dati dopo la loro comunicazione all'autorità giudiziaria.

15.8. *Servizi telefonici non richiesti*

Anche nell'anno di riferimento sono pervenuti al Garante numerosi reclami, segnalazioni e quesiti con i quali sono state lamentate ripetute violazioni del diritto al corretto e lecito utilizzo dei dati personali nella prestazione di alcuni servizi di comunicazione elettronica da parte, oltre che dei fornitori di servizi, anche dei rivenditori dislocati sul territorio. In particolare sono state evidenziate violazioni connesse all'indebita attivazione di contratti, schede o servizi telefonici non richiesti dagli interessati; in alcuni casi, soggetti cui erano state intestate falsamente schede di telefonia mobile senza consenso si sono trovati addirittura coinvolti in indagini penali.

Le segnalazioni pervenute hanno riguardato anche ulteriori problematiche legate alla selezione automatica dell'operatore e all'attivazione di servizi non richiesti, tra i quali segreterie telefoniche e collegamenti Internet a banda larga.

L'ampia portata del fenomeno risulta, peraltro, anche dalla trattazione di diversi ricorsi presentati all'Autorità, la quale da tempo si occupa della tematica, avendo svolto negli anni passati (*v. Relazione* 2003, pp. 87 e 140), anche impegnativi accertamenti di carattere ispettivo.

Sulla base delle informazioni acquisite, anche in occasione di nuovi accertamenti ispettivi effettuati presso alcuni tra i maggiori operatori telefonici, il Garante ha effettuato un'apposita istruttoria al fine di intervenire sul fenomeno con un provvedimento di carattere generale volto ad individuare un quadro di garanzie che assicuri il rispetto dei diritti e delle libertà fondamentali dei cittadini.

Nel *provvedimento* adottato il 16 febbraio 2006 ([doc. *web* n. 1242592], in *G.U.* 6 marzo 2006, n. 54), il Garante ha quindi imposto agli operatori telefonici la predisposizione di procedure che consentano di rilevare tempestivamente le intestazioni multiple di schede telefoniche prepagate ad una medesima persona. In particolare, quando le intestazioni siano superiori a 4 (per le persone fisiche) e a 7 utenze (per le società) l'operatore dovrà chiederne espressa conferma all'intestatario. Resta vietato attivare servizi senza aver acquisito l'espresso consenso preventivo degli interessati; inoltre, le persone vanno contattate per finalità pubblicitarie o promozionali solo se hanno manifestato uno specifico e preventivo consenso a ricevere a tal fine chiamate e comunicazioni. Gli addetti ai *call center* devono, al momento del contatto, spiegare agli interessati da dove siano stati estratti i dati che li riguardano. Deve essere, inoltre, registrata immediatamente e rispettata la volontà di non ricevere il servizio, nonché l'eventuale contrarietà espressa in relazione all'uso dei dati.

Il Garante ha inoltre imposto ad operatori telefonici, di comunicazione elettronica e *call center* di verificare attentamente, anche attraverso controlli a campione,

l'attività di rivenditori e incaricati, allo scopo di rintracciare immediatamente chi materialmente abbia effettuato eventuali attivazioni indebite.

15.9. *Informativa con modalità diverse da quelle ordinarie*

Nel mese di dicembre dell'anno di riferimento l'Autorità ha ricevuto la richiesta di un operatore telefonico volta a consentire di informare gli interessati in modo diverso da quello ordinario ai sensi dell'art. 13 del Codice.

La richiesta riguardava un progetto di fusione per incorporazione (avvenuta poi nei primi mesi del 2006) tra la società istante ed un altro operatore, del quale la prima ha acquisito il complesso aziendale con tutti i rapporti giuridici attivi e passivi in atto, assumendo di conseguenza la qualità di titolare del trattamento dei dati personali dei relativi interessati. All'esito dell'istruttoria sono state individuate modalità di informazione sostitutive di quelle rivolte, caso per caso, a ciascun interessato, con particolare riguardo alle caratteristiche, anche comunicative, del contenuto dell'avviso da pubblicare sugli organi di stampa.

15.10. *Il codice deontologico*

La prossima definizione del codice deontologico per gli operatori Internet consentirà di introdurre, in un settore in continua evoluzione, specifiche garanzie al cui rispetto sarà subordinata la liceità e la correttezza dei diversi trattamenti di dati personali (art. 12, comma 3, del Codice). L'obiettivo principale è indicare soluzioni effettive, adeguate e dinamiche ad alcune questioni relative al trattamento dei dati personali *on-line* che possano, da un lato, sensibilizzare maggiormente gli utenti in rete sui rischi in materia correlati all'uso di Internet, offrendo loro ulteriori opportunità di tutela e, dall'altro, indicare ai diversi operatori interessati concreti strumenti per adempiere agli obblighi di legge (anche per quanto riguarda i principi di cui all'art. 11 del Codice) assicurando un più elevato livello di rispetto della normativa sulla protezione dei dati personali.

In questa prospettiva sono proseguiti nel 2005 gli incontri nel tavolo di lavoro composto dagli operatori del settore –rappresentati dalle relative organizzazioni di categoria– e dalle associazioni dei consumatori che hanno entrambi aderito all'invito a parteciparvi rivolto dall'Autorità.

In tale ambito sono state affrontate diverse esigenze fra le quali quelle relative: all'obbligo di informare adeguatamente gli utenti circa i possibili trattamenti, impliciti o espliciti, che possono riguardarli; al consenso da manifestare espressamente e liberamente; ai presupposti e ai limiti entro i quali è legittimo l'uso di marcatori o dispositivi analoghi *on-line*; alle modalità semplificate per esercitare i diritti di cui all'art. 7 del Codice; ai trattamenti che possono presentare rischi specifici per la sicurezza degli utenti in rete, come nel caso del *phishing*; allo *spamming*, con particolare riferimento alla possibilità di individuare misure di filtraggio a tutela degli interessati. Il gruppo di lavoro ha poi riscontrato l'opportunità di affrontare altri temi impegnativi quali quello del trattamento dati rispetto ai nomi a dominio, al diritto all'oblìo in rete e, quindi, alle garanzie rispetto ai motori di ricerca.

Alla luce dei vari contributi e delle riflessioni svolte, il tavolo redigerà una prima bozza di codice deontologico che sarà pubblicata sul sito Internet dell'Autorità per una consultazione pubblica. Sulla base delle osservazioni e proposte che perverranno, il tavolo apporterà le eventuali modifiche al testo che, sottoposto all'esame

dell'Autorità e da questa "certificato" in conformità alle procedure in tema di codici deontologici in fase di generale formalizzazione, verrà trasmesso al Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* e la sua allegazione al Codice sulla protezione dei dati personali.

15.11. *Motori di ricerca e diritto all'oblìo*

La problematica relativa al *cd.* "diritto all'oblìo", ossia il diritto ad "essere dimenticato" nella dimensione pubblica o, comunque, non più privata, precedentemente acquisita, presenta profili di particolare complessità laddove le informazioni personali che si intendano cancellare siano state diffuse in Internet. Inserendo nei motori di ricerca più comuni alcune parole chiave è infatti particolarmente agevole risalire in tempo reale ad un numero considerevole di informazioni di carattere personale riguardanti una stessa persona e riferite ad epoche assai diverse.

Questa efficiente profilazione generalizzata può porsi in conflitto con il diritto di un soggetto interessato a veder delimitata nel tempo la diffusione indifferenziata di molte informazioni che lo riguardano, che può non essere più giustificata alla luce delle finalità e delle circostanze originarie; ciò, senza considerare i casi nei quali le informazioni pubblicate risultino sin dall'inizio non corrette o, comunque, incomplete o non aggiornate.

In questo quadro diversi interessati contestano spesso la circostanza che le copie *cache* (e le relative sintesi) –attraverso le quali i motori di ricerca mettono a disposizione degli utenti le pagine *web* indicizzate contenenti le parole chiave utilizzate nelle ricerche– non riportano automaticamente le modifiche già intervenute nelle pagine *web* dei "siti sorgente", anche quando queste ultime siano state modificate o cancellate da diverso tempo. I motori di ricerca non procedono infatti ad una revisione automatica ed immediata dei propri indici a fronte della modifica dei siti richiamati, bensì effettuano aggiornamenti periodici degli stessi attraverso l'utilizzo di un *software* (*cd. crawler*).

Sul ruolo dei motori di ricerca, è stata pertanto avviata una specifica riflessione da parte dell'Autorità, anche alla luce dei numerosi ricorsi e segnalazioni pervenuti.

Fra questi ultimi merita menzione almeno un ricorso proposto nei confronti di Google Italy S.r.l.. In tale occasione, il Garante, con una decisione intervenuta poi di recente, ha infine riconosciuto in capo al motore di ricerca un'autonoma titolarità del trattamento, consistente nella creazione e nella conservazione di cosiddette copie *cache* di pagine *web* pubblicate sul sito sorgente. Tuttavia, non risultando provato che il trattamento contestato fosse effettuato da un soggetto stabilito sul territorio dello Stato, l'Autorità si è riservata di esaminare, nell'ambito di una distinta attività, le questioni relative alla tutelabilità dei diritti dell'interessata in rapporto a titolari situati all'estero (nella specie, Google Inc. avente sede negli Stati Uniti). A tal fine, è stata sollecitata una fattiva collaborazione con tale società, per individuare nel breve periodo soluzioni concrete che permettano di garantire pienamente sul territorio italiano i diritti e le libertà fondamentali degli interessati, anche quando gli strumenti utilizzati per il trattamento siano situati in Paesi non appartenenti all'Unione europea (*cfr. Comunicato stampa* 13 aprile 2006; sulla tematica, *v.* anche quanto riportato al par. 18.3).

15

15.12. *Televisione digitale: i servizi interattivi*

Nel 2005 l'Autorità ha adottato un provvedimento generale (*Provv.* 3 febbraio 2005 [doc. *web* n. 1109503]) con il quale ha prescritto ai fornitori dei servizi televisivi interattivi di adottare misure necessarie per conformare i loro trattamenti alle disposizioni in materia di protezione dei dati personali. Il provvedimento si è reso necessario per evitare eventuali forme invasive di controllo sulle abitudini delle persone ed operazioni illecite di profilazione, oltre che per garantire ad utenti ed abbonati una piena consapevolezza sui trattamenti di dati personali che li riguardano, anche al fine di esercitare liberamente le loro scelte ed i loro diritti, senza essere pregiudicati nella fruizione di servizi e di opportunità.

La circostanza che la televisione digitale interattiva trovi usuale utilizzo in un ambito segnatamente "privato", quale quello familiare, richiedeva particolare attenzione da parte del Garante. In tali contesti, l'utente nutre la ragionevole aspettativa di essere al riparo da forme di controllo; spesso, poi, ad uno stesso apparecchio televisivo possono corrispondere più fruitori differenziati (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi tutti in grado di compiere liberamente le loro scelte, senza che ciò comporti schedature o profilazioni.

Nello scorso anno si è registrato un aumento sensibile del numero degli utenti e degli operatori del settore (a prescindere dalla tecnica di trasmissione impiegata, che può implicare l'utilizzo del satellite, del cavo o del digitale terrestre), unitamente a novità tecnologiche che possono presentare nuovi rischi o, comunque, profili di interesse per la sfera privata degli interessati.

Nel richiamato provvedimento l'Autorità ha pertanto prescritto agli operatori del settore le misure di carattere generale volte a garantire il rispetto dei principi di necessità, liceità, correttezza e proporzionalità. In primo luogo, occorre ridurre al minimo l'utilizzo delle informazioni relative ad abbonati e utenti identificabili, privilegiando l'uso di dati anonimi (come schede prepagate). In questo caso, anche l'acquirente del *decoder* digitale terrestre deve essere anonimo, ferma restando la necessità di prender nota del nome al solo fine di evitare un'attribuzione multipla del relativo contributo statale. Si prefigura diversamente, invece, il caso del rapporto contrattuale che debba intercorrere necessariamente con un abbonato identificato. Resta poi ferma l'illiceità di eventuali banche dati di titolari di antenne televisive o satellitari (il cosiddetto "catasto delle antenne").

Profilazione

Quanto, poi, alla profilazione attraverso la tv interattiva, il Garante ha stabilito che non è lecito trattare dati personali quali quelli relativi a tempi di connessione, visioni di programmi ed eventi, nonché ad analisi del comportamento in presenza di spazi pubblicitari, a meno che l'interessato, debitamente informato, non abbia prestato il proprio consenso libero e specifico. In tal caso, i dati di dettaglio su acquisti e servizi possono essere tuttavia conservati per un periodo comunque non superiore a dodici mesi dalla loro registrazione, salva la loro trasformazione in forma anonima. Le eventuali intenzioni di trattare i dati oltre tali termini possono essere attuate solo previa valutazione preliminare dell'Autorità ai sensi dell'art. 17 del Codice.

Sondaggi e ricerche di mercato

Con riguardo ai sondaggi, alle ricerche di mercato e alle altre ricerche campionarie, il fornitore deve adottare una tecnica che separi il voto espresso dal nominativo di chi ha partecipato al sondaggio; laddove la commistione risulti tecnicamente inevitabile, deve rendere le risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali.

Non è di regola ammesso il trattamento di dati sensibili, né per l'ordinaria pre-

stazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, a meno che tale trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che consentito dall'interessato in forma scritta o telematica equiparabile allo scritto.

Informativa

L'Autorità ha, poi, prescritto ai gestori di servizi televisivi l'obbligo di fornire informative più chiare e complete, prevedendo anche l'inserimento, prima di ogni acquisto o altro tipo di rapporto interattivo, di un'apposita schermata-video. Il consenso può essere manifestato anche elettronicamente attraverso il telecomando e deve essere libero da qualsiasi condizionamento. In caso di fatturazione degli acquisti (*ad es.* di partite o film), l'abbonato deve avere la possibilità di non ricevere una fatturazione dettagliata. Gli acquisti devono essere indicati per importo totale, data e costo, mentre vanno forniti i "titoli" specifici solo su richiesta.

L'Autorità ha poi imposto agli operatori di indicare nell'informativa il termine di conservazione dei dati dopo la cessazione del rapporto (termine che non può essere comunque superiore ad un trimestre, salvi eventuali obblighi di legge specifici sulla conservazione di documentazione contabile), nonché di predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi ai quali gli stessi siano stati eventualmente comunicati.

Verifica preliminare

Il Garante ha inoltre previsto in capo ai fornitori dei servizi televisivi interattivi l'obbligo di richiedere la verifica preliminare ai sensi dell'art. 17 del Codice laddove il trattamento di dati consista nella "*richiesta –rivolta dal fornitore ai singoli utenti– di identificarsi nominativamente al momento in cui essi inviano informazioni attraverso il canale di ritorno*". Ciò, al fine di poter prescrivere specifici accorgimenti e misure a garanzia degli interessati, nei casi in cui all'utente (persona fisica eventualmente diversa dall'abbonato) sia richiesto di essere individuato specificamente nel momento in cui compia un'operazione diversa da quelle effettuabili "ordinariamente" nel quadro del comune svolgimento di un rapporto. A tale riguardo sono già pervenute all'Autorità alcune richieste di valutazione preliminari sulle quali il Garante è in procinto di pronunciarsi caso per caso.

È stata infine avviata una complessa attività ispettiva volta a verificare il corretto e completo adeguamento degli operatori alle prescrizioni impartite dall'Autorità in materia.

15.13. Pornosquatting

Sono pervenute a questa Autorità diverse segnalazioni con le quali è stata lamentata la violazione del diritto all'immagine, al nome ed alla professionalità, commessa presso alcuni siti Internet a contenuto pornografico. I segnalanti lamentano in particolare che, digitando il loro nome su un qualsiasi motore di ricerca, compaiono, fra i risultati, anche alcuni indirizzi di siti pornografici che associano al loro nome contenuti osceni e denigratori della reputazione.

Da alcune ricerche preliminari curate da questa Autorità, si è potuto verificare che i casi di specie rientrano nel fenomeno, diffuso in Internet, meglio noto come "*pornosquatting*" che consiste nell'inserire nomi di personaggi famosi, o di noti marchi, tra le parole chiave riscontrabili nei *cd.* "*meta-tag*" (stringhe ipertestuali) della pagina *web*, che dovrebbero descrivere essenzialmente il contenuto del sito.

Tale pratica risulta piuttosto lesiva degli interessati in quanto la tecnologia dei motori di ricerca imposta le ricerche proprio in base alle parole contenute in tali stringhe ipertestuali. Di conseguenza, se si cercano in rete notizie relative ad un

determinato soggetto e il suo nome è contenuto nei "*meta-tag*" di un sito *web*, l'indirizzo di quest'ultimo verrà sicuramente presentato tra i risultati dal motore di ricerca interrogato.

La circostanza che i titolari dei siti pornografici utilizzino nomi di personaggi noti per rendere maggiormente "reperibili" gli indirizzi dei siti stessi può peraltro essere considerata alla stregua di uno sfruttamento illegittimo della notorietà delle persone coinvolte, oltre che un'induzione in errore degli utenti.

L'Autorità sta ultimando, anche avvalendosi della collaborazione della Guardia di finanza, i necessari accertamenti preliminari.

15.14. Rfid

In un *provvedimento* del 9 marzo 2005 [doc. *web* n. 1109493] il Garante ha impartito prescrizioni specifiche per chi intenda produrre ed utilizzare le cosiddette "etichette intelligenti", minuscoli *chip* a radiofrequenza (*Radio Frequency Identification-Rfid*) attivati da lettori ottici, che hanno iniziato a trovare applicazione anzitutto nell'ambito di aziende, esercizi commerciali e della grande distribuzione per ottenere alcuni vantaggi, a volte anche per il consumatore (migliore gestione di prodotti aziendali, maggiore rapidità di operazioni commerciali, agevole rintracciabilità dell'origine di particolari prodotti e controllo degli accessi a luoghi riservati).

Alcuni utilizzi di questa tecnologia –che non si limitino a tracciare un prodotto per garantire l'efficienza del processo di produzione industriale– possono comportare anche una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone. Con l'uso di *Rfid* si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori a fini di profilazione ed essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usano, indossano o trasportano.

I sistemi *Rfid* possono essere impiegati da soggetti pubblici o privati anche ad altri scopi quali l'identificazione personale o la tutela della salute. Alcuni particolari usi come l'impianto di *microchip* sottopelle hanno già sollevato problematiche di grande delicatezza. Ulteriori pericoli possono derivare dall'adozione di *standard* comuni in materia, tali da favorire la possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (*ad es.*, mediante la loro riscrittura). I rischi possono accrescersi nel caso in cui si integrino le tecniche *Rfid* con infrastrutture di rete avvalendosi della telefonia e di Internet, e sulla base dello stesso sviluppo tecnologico che, potenziando i sistemi, potrebbe consentire una "lettura" delle etichette a distanze sempre maggiori.

Il provvedimento generale si collega a quello varato nello stesso periodo dal Gruppo art. 29, allo scopo di stabilire alcune misure per rendere conformi l'impiego dei sistemi *Rfid* alle norme sulla *privacy* nei casi in cui si trattino dati personali relativi a persone identificate o identificabili, e tutelare la loro dignità e la libertà.

Informativa

In particolare, l'Autorità ha prescritto che gli interessati siano adeguatamente informati dell'utilizzo di sistemi *Rfid,* così come dell'esistenza dei lettori ottici che attivino l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche *Rfid* sono utilizzate non esime, peraltro, dall'apporre un'informativa più specifica in relazione agli stessi oggetti e prodotti che recano le etichette intelligenti.

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

L'utilizzo delle *Rfid* che comporta un trattamento di dati personali può avvenire

solo con il consenso espresso e specifico degli interessati, a meno che ricorra uno degli altri presupposti di legge; il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato.

Rfid e profilazione

Se le etichette intelligenti sono associate all'utilizzo di carte di fedeltà, e si trattano dati a fini di profilazione dei consumatori, occorre informare ed acquisire il consenso degli interessati; il consenso non è invece necessario quando le etichette intelligenti sono adoperate solo per modalità di pagamento e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili.

Deve comunque essere garantito comunque il diritto di asportare, disattivare o interrompere gratuitamente ed in maniera agevole il funzionamento delle *Rfid* al momento dell'acquisto del prodotto sui cui è apposta l'etichetta. Le etichette devono essere posizionate in modo tale da risultare facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto (*ad es.*, collocate solo sulla confezione); non è, di regola, lecita l'installazione di *Rfid* destinate a rimanere attive oltre la barriera-cassa dell'esercizio commerciale.

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

L'avvio di trattamenti di dati che indichino la posizione geografica di persone o oggetti mediante reti di comunicazione elettronica o che siano effettuati allo scopo di costruire profili o personalità di un individuo deve essere, inoltre, comunicato preventivamente al Garante.

Impianto di *microchip* sottopelle

Il Garante ha inoltre ritenuto che l'impianto di *microchip* sottopelle debba essere in via di principio escluso in quanto contrastante con i diritti, le libertà fondamentali e la dignità della persona. Tali impianti sono limitatamente ammissibili, in casi eccezionali, per comprovate e giustificate esigenze di tutela della salute delle persone. L'interessato, comunque, deve poter ottenere la rimozione del *microchip* e l'interruzione del relativo trattamento dei dati che lo riguardano; si devono inoltre prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato. Il Garante ha stabilito infine che i soggetti che intendono utilizzare tali *microchip* devono sottoporre i relativi sistemi alla verifica preliminare dell'Autorità.