venditore/fornitore dei beni o servizi oggetto del contratto), ne verrà fatta opportuna annotazione.

Tra i partecipanti ai sistemi non figurano le società di telefonia, che avevano iniziato a collaborare con le centrali rischi in termini che il Garante aveva già considerato illegittimi. Il principio è stato ribadito anche in un provvedimento a seguito di ricorso (v. *Newsletter* 20-26 dicembre 2004), nel quale è stato precisato che nei sistemi di informazioni creditizie (Sic) potranno figurare solo dati relativi al vero e proprio rischio creditizio e non informazioni relative a bollette telefoniche non pagate e contratti di telefonia.

Il bilanciamento di interessi

Il trattamento dei dati personali nei sistemi di informazione creditizia richiede, secondo le previsioni del Codice, il consenso libero e informato degli interessati (art. 23) o la sussistenza degli altri presupposti di liceità alternativi rispetto ad esso (art. 24).

In proposito, l'Autorità ha ritenuto opportuno dare attuazione all'istituto del bilanciamento di interessi (previsto all'art. 24, comma 1, lett. *g*), del Codice), individuando i casi in cui il predetto trattamento potrà avvenire anche a prescindere dal consenso dell'interessato ed al solo fine di perseguire i legittimi interessi del titolare del trattamento o dei terzi destinatari dei dati (*Provv.* 16 novembre 2004, in *Documentazione* par. 40).

Il provvedimento del Garante riguarda in particolare i trattamenti relativi a:

- ritardi nel pagamento di un credito (che possono essere conservati, a seconda dei casi, per dodici o ventiquattro mesi dalla loro regolarizzazione);
- rapporti di credito per i quali si sono verificati ritardi o inadempimenti non regolarizzati (che possono essere conservati per non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto, o comunque dalla data di cessazione del rapporto). In quest'ultimo caso, possono essere conservati ulteriormente anche i dati personali relativi ad informazioni creditizie di tipo positivo eventualmente presenti nel sistema informativo, anche se riferiti ad altri rapporti di credito riguardanti il medesimo interessato.

In questi casi, il trattamento dei dati personali da parte dei soggetti che gestiscono o consultano sistemi di informazioni creditizie, è lecito ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, anche in assenza del consenso degli interessati.

Dati provenienti da fonti pubbliche

Secondo un principio recepito anche nel nuovo codice di deontologia, i dati trattati nell'ambito dei sistemi di informazioni creditizie devono essere in ogni caso di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalità perseguite, oltre che relativi ad una richiesta/rapporto di credito. Non è sufficiente, a tal riguardo, che le informazioni vengano acquisite da fonti pubbliche (che comunque, se registrate, dovranno figurare in banche dati separate dal sistema di informazioni creditizie).

Al riguardo, si segnala un ricorso presentato da un cittadino relativamente alla mancata cancellazione, da parte del gestore del sistema di informazioni creditizie, di dati personali relativi alla trascrizione di una sentenza di divisione ereditaria e contenuti nella banca dati denominata "Atti pubblici". Il gestore giustificava il proprio diniego adducendo la perfetta coincidenza tra le informazioni censite nella propria banca dati e quelle risultanti dalla conservatoria dalla quale erano tratte, non ritenendo quindi di poter procedere alla cancellazione perché si era limitato a *"veicolare quanto contenuto nelle banche dati pubbliche consultate"* (*Provv.* 18 ottobre 2004). L'Autorità ha ritenuto il ricorso fondato in quanto, pur non contestandosi l'esattezza dell'informazione, il suo inserimento in una banca dati relativa a "dati pregiudizievoli" ha dato luogo ad un trattamento non corretto ai sensi dell'art. 11, comma 1,

lett. *a*), del Codice, per il fatto di aver descritto arbitrariamente come dato negativo un'informazione neutra quale quella connessa ad un'ordinaria operazione di scioglimento di una comunione ereditaria.

È stato al contrario ritenuto lecito il trattamento relativo ad un pignoramento immobiliare in quanto l'informazione, ancora presente nel pubblico registro dal quale era stata tratta, risultava pertinente e necessaria, trovando applicazione nel caso di specie la disposizione del Codice per cui, nel caso di informazioni provenienti da pubblici registri, i soggetti privati possono effettuare il relativo trattamento anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*), *Provv.* 29 aprile 2004).

Contributo spese

Nel quadro dei lavori relativi ai sistemi di informazione creditizia l'Autorità ha poi adottato il 23 dicembre 2004 una prima deliberazione di applicazione dell'art. 10, comma 8, del Codice, per il solo 2005, su istanza di una società che ha chiesto di riconoscere la facoltà di esigere dagli interessati un contributo spese per l'esercizio di alcuni diritti, in relazione alla situazione straordinaria che, presso quella società (Crif S.p.A.), si è temporaneamente determinata in ragione del notevole impiego di mezzi connessi alla complessità ed entità delle ricerche conseguenti alla richieste (*Deliberazione* 23 dicembre 2004, n. 15).

9.3. *Archivio degli assegni bancari e postali e delle carte di pagamento irregolari*

Anche il contenzioso relativo alle segnalazioni effettuate da soggetti pubblici (autorità giudiziaria e Ministero dell'interno) e privati (banche, uffici postali, società emittenti carte di credito) all'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (Cai-Centrale d'allarme interbancaria) ha registrato un notevole incremento, con la proposizione di numerosi ricorsi da parte di privati cittadini concernenti la mancata cancellazione o rettifica dei dati.

Come ricordato nelle precedenti relazioni, l'archivio risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti e in esso vengono segnalati i provvedimenti o le segnalazioni riguardanti persone che hanno emesso assegni senza autorizzazione o provvista, titolari di carte di pagamento revocate (per mancato pagamento o costituzione di fondi), nonché assegni o carte di pagamento sottratti, smarriti o bloccati. Gli enti che effettuano tali segnalazioni vi sono obbligati da precise norme di legge (v. legge 15 dicembre 1990, n. 386, legge 25 giugno 199, n. 205, d.lg. 30 dicembre 1999, n. 507) che non consentono ai segnalanti alcuno spazio di valutazione personale.

Con alcune decisioni il Garante ha esaminato taluni profili relativi al trattamento dei dati effettuato presso tale archivio, riconoscendo la possibilità di esercitare il complesso dei diritti previsti dall'art. 7 del Codice sia nei confronti degli intermediari segnalanti sia della Banca d'Italia, soggetti che agiscono entrambi in qualità di titolari dei trattamenti rispettivamente effettuati (*Provv.* 27 settembre 2004 e 4 ottobre 2004).

L'Autorità ha altresì dichiarato l'infondatezza di diverse richieste volte ad ottenere la cancellazione di alcuni dati personali dall'archivio Cai relativi alla revoca di carte di credito o dell'autorizzazione ad emettere assegni, in quanto tali segnalazioni risultavano essere state effettuate nel rispetto della vigente normativa che disciplina il funzionamento del Cai (art. 10-*bis*, l. n. 386/1990; v. *Provv.* 4 e 12 ottobre 2004).

Anche un pagamento tardivo ritenuto satisfattivo dal creditore, ma non documentato nelle forme puntualmente previste dalla legge (art. 8, l. n. 386/1990), deve essere infatti segnalato nell'archivio una volta decorso il termine di legge indicato nel preavviso di revoca dell'autorizzazione ad emettere assegni a causa del mancato

pagamento per difetto di provvista. Resta in ogni caso salva, per effetto del Codice, la possibilità per gli interessati di richiedere ed ottenere la rettifica della segnalazione a loro carico, allorché siano in grado di dimostrare l'avvenuto pagamento nelle forme idonee, attraverso, ad esempio, un'integrazione della documentazione richiesta dalla legge (*Provv.* 4 ottobre 2004).

In applicazione di questi principi, è stato ritenuto fondato il ricorso di un imprenditore che era stato privato dell'autorizzazione ad emettere assegni per non essere riuscito a dimostrare alla banca, seguendo le prescritte formalità, di aver pagato un assegno. L'Autorità, pur riconoscendo la sussistenza dei presupposti per l'inserimento del nominativo dell'imprenditore nell'archivio informatizzato, ha tuttavia ordinato la cancellazione dei dati inseriti nell'archivio, in quanto gli stessi documentavano una situazione non più corrispondente alla realtà: l'interessato figurava infatti come un soggetto che non aveva provveduto al pagamento, neppure tardivo, dell'assegno, mentre lo stesso era stato effettuato per intero, anche se la documentazione in grado di dimostrarlo non era stata inizialmente accettata e, infine, era giunta con lieve ritardo (*Provv.* 27 settembre 2004). Non si è ritenuta, quindi, giustificata la tesi sostenuta dai titolari del trattamento di dover conservare i dati nella Cai per il periodo di efficacia del provvedimento di revoca dell'autorizzazione ad emettere assegni (sei mesi) sulla base di un regolamento (d.m. n. 458/2001), normativa peraltro di rango secondario rispetto al Codice, che disciplina in termini generali la conservazione dei dati.

9.4. *Trattamenti in ambito assicurativo*

Accesso alle perizie medico-legali

Nel contesto assicurativo il tema delle perizie medico-legali è da tempo al centro di un intenso contenzioso e continua ad essere oggetto di numerose decisioni del Garante.

La questione dell'accesso ai dati personali contenuti in perizie medico-legali redatte da professionisti incaricati dalle compagnie assicurative di stimare i danni denunciati dagli assicurati –rispetto alla quale in passato si erano registrate alcune difformità di posizioni tra Garante e taluna giurisprudenza di merito– è ora oggetto di una apposita e dettagliata disposizione del Codice (art. 8, comma 4) in base alla quale *"l'esercizio dei diritti di cui all'art. 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento"*.

In alcune decisioni su ricorsi, il Garante ha ricordato che, come molti altri documenti, anche le perizie medico-legali in ambito assicurativo contengono di regola dati personali del paziente interessato, sia nella parte nella quale sono riportati dati identificativi dello stesso, nonché riscontri di visite mediche e dei cd. esami obiettivi, sia all'interno della parte che comprende valutazioni e giudizi del perito fiduciario. Informazioni personali riferite all'interessato possono essere ugualmente presenti nelle relazioni investigative eventualmente predisposte su incarico delle imprese di assicurazione. Si tratta infatti di informazioni comunque relative all'interessato che devono essere considerate "dati personali" ai sensi dell'art. 4, comma 1, lett. *d*), del Codice.

È possibile comunque che il titolare del trattamento invochi il temporaneo differimento dell'esercizio dei diritti di cui all'art. 7 del Codice, per il solo periodo durante il quale potrebbe derivarne un pregiudizio per lo svolgimento di cd. "inda-

gini difensive" o, più in generale, per far valere o difendere un diritto in sede giudiziaria (art. 8, comma 2, lett. *e*) del Codice); la valutazione dell'esistenza del pregiudizio deve essere effettuata caso per caso e sulla base di elementi concreti. Cessate tali circostanze, il diritto di accesso ai dati personali può essere nuovamente esercitato (*Provv.* 19 aprile 2004).

Per quanto riguarda le modalità del riscontro alle richieste di accesso relative ai dati inerenti allo stato di salute, contenuti nella perizia medico-legale, esso deve essere fornito direttamente agli interessati (a differenza di quanto previsto dalla normativa precedente, in base alla quale il riscontro doveva invece provenire da un medico di fiducia designato dal titolare o dall'interessato: v. l'art. 23, comma 2, della legge n. 675/1996, abrogato). L'art. 84 del Codice prevede ora l'obbligo del loro inoltro per il tramite del medico di fiducia solo a carico di esercenti le professioni sanitarie e di organismi sanitari.

Liceità e correttezza del trattamento in ambito assicurativo

Sempre in ambito assicurativo, ulteriori interventi dell'Autorità hanno riguardato alcuni profili relativi al trattamento di dati sensibili degli assicurati o di terzi.

In particolare, valutando la modulistica predisposta da una compagnia assicurativa, è stato affrontato il profilo dell'informativa. In tale occasione, il Garante, oltre a ribadire che la disciplina sulla protezione dei dati personali rende comunque necessaria la raccolta da parte dell'impresa di assicurazione del consenso scritto dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute (v. art. 26, del Codice, nonché le autorizzazioni del Garante nn. 2 e 5 del 2004), ha richiamato l'attenzione della società sulla necessità che il modello di informativa sottoposto ai clienti, e più in generale agli interessati, specifichi con chiarezza le caratteristiche del trattamento. In particolare, anche in considerazione del fatto che il consenso dell'interessato deve essere prestato *"specificamente in riferimento ad un trattamento chiaramente individuato"* (art. 23, comma 3, del Codice), l'informativa deve contenere un'indicazione puntuale e non esemplificativa dei titolari in favore dei quali il consenso potrebbe valere, eventualmente allegando un elenco, nonché delle principali caratteristiche degli ulteriori trattamenti effettuati (finalità, modalità e ambito di comunicazione dei dati).

La società è stata inoltre invitata a valutare la praticabilità di una designazione del professionista che effettua le visite medico-legali su incarico della stessa, in qualità di "responsabile del trattamento" ai sensi dell'art. 29 del Codice, specificando analiticamente per iscritto i compiti e le istruzioni cui attenersi. In tal modo il professionista potrebbe rendere l'informativa all'interessato precisando che i dati rientreranno nell'ambito del più generale trattamento effettuato dall'impresa di assicurazioni. In mancanza di tale designazione il professionista deve essere considerato un autonomo titolare del trattamento, anche relativamente ai dati sensibili rilevati nel contesto della visita medico-legale, e deve pertanto effettuare una autonoma informativa all'interessato e riceverne il consenso formulato per iscritto.

L'Autorità ha esaminato, inoltre, una segnalazione relativa ad un contratto di assicurazione riguardante il rimborso della penale prevista per l'annullamento di un viaggio; nel caso di specie, la compagnia di assicurazioni non ha proceduto al rimborso perché non ha reputato sufficiente il certificato medico inviato dal segnalante e riferito ad un congiunto impossibilitato a partecipare al viaggio, richiedendo, invece, copia della cartella clinica attestante la ragione dell'addotta impossibilità.

In tale occasione, il Garante non ha ritenuto ammissibile l'acquisizione, da parte del segnalante o di altri soggetti (la compagnia assicuratrice), della cartella clinica detenuta dalla struttura ospedaliera presso cui la persona interessata era stata ricove-

rata. Si è infatti rilevato che, quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il medesimo è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile (art. 60 del Codice; si vedano anche i chiarimenti sul concetto di "diritto di pari rango" forniti dal Garante con provvedimento del 9 luglio 2003, con cui è stato precisato che, quantomeno "nella prevalenza dei casi", i diritti di credito non rientrano tra i "diritti di rango almeno pari" a quello della persona cui si riferiscono i dati).

Preso atto che il diritto fatto valere dal segnalante nei confronti della società assicuratrice aveva natura di mero diritto di credito (rimborso della penale pagata al *tour operator* in seguito all'annullamento del viaggio), l'Autorità ha concluso per l'impossibilità per la struttura ospedaliera di accogliere una sua eventuale richiesta di ottenere, a scopo di tutela di tale diritto, un accesso ai dati sanitari contenuti nella cartella clinica del terzo ricoverato.

Già in precedenti occasioni il Garante aveva considerato giustificati i trattamenti di dati relativi alla salute degli assicurati effettuati da imprese di assicurazione al fine della gestione e dell'esecuzione di polizze infortuni e malattie, previa acquisizione del consenso scritto dell'interessato (nel caso di specie, peraltro, estraneo al contratto). Tra questi trattamenti può rientrare anche la raccolta di dati sanitari contenuti in cartelle cliniche degli assicurati, quando tali dati siano strettamente necessari per fornire le specifiche prestazioni richieste dagli interessati con questa tipologia di contratti, in relazione –ad esempio– ad attività di accertamento dei sinistri denunciati e di rimborso delle spese mediche sostenute dall'assicurato (cfr. *Provv.* 12 aprile 1999, in *Bollettino* n. 8 del 1999, p. 42).

È stato sottolineato, anzi, che anche per il trattamento dei dati contenuti nella certificazione sanitaria già inviata dal segnalante la società assicuratrice avrebbe dovuto comunque acquisire il consenso scritto della persona interessata. Inoltre, la raccolta ed il trattamento dei dati sanitari devono comunque essere effettuati in conformità ai principi di indispensabilità, di pertinenza e di non eccedenza dei dati rispetto alle finalità perseguite (v. l'art. 11 del Codice) oltre che ai requisiti indicati dalle citate autorizzazioni generali, con particolare riguardo alla stretta necessità per la società di assicurazione di acquisire copia integrale di una cartella clinica ai fini della liquidazione di un sinistro. L'acquisizione dell'intera cartella clinica può infatti rivelarsi non rispettosa dei principi ora richiamati poiché tale documento, insieme ad elementi strettamente necessari ai fini delle verifiche effettuate dall'impresa di assicurazione per procedere al rimborso (riguardo, ad esempio, ad informazioni che permettono di stabilire la natura della malattia), contiene ulteriori dati di carattere sanitario che possono non avere alcuna rilevanza ai fini delle suddette verifiche e che devono essere quindi omesse.

Oltre ad aver rilasciato nuove autorizzazioni generali, alcune delle quali di diretto rilievo per il settore assicurativo (v. in particolare le autorizzazioni nn. 2 e 5 del 2004), il Garante ha autorizzato con un provvedimento *ad hoc* una società cooperativa di assicurazioni che ne aveva fatto richiesta, a trattare i dati relativi alla convinzione religiosa dei propri soci (*Newsletter* 4-10 ottobre 2004). L'autorizzazione riguarda i dati e le operazioni strettamente indispensabili per l'applicazione di una specifica norma dello statuto della compagnia di assicurazioni, alle stesse condizioni previste dalla citata autorizzazione generale n. 5/2004 (che la società deve già rispettare per il trattamento degli altri dati personali dei propri assicurati).

Nell'accogliere la richiesta dell'assicurazione, il Garante ha tenuto conto anche dello scopo mutualistico della società che offre ai propri soci contratti di assicura-

zione a condizioni economiche particolari. La società cooperativa di assicurazioni si trova, secondo quanto stabilito dallo statuto, nella condizione di raccogliere e conservare anche dati dei soci che dichiarano di professare la religione cattolica e manifestano sentimenti di adesione alle opere cattoliche. A differenza degli altri clienti, tali soci possono essere assicurati a particolari condizioni di favore.

Nel caso in esame, l'intervento specifico a tutela del dato "religioso" dei soci si è reso necessario, non essendo prevista nelle autorizzazioni generali una disposizione che regoli espressamente il trattamento di questo tipo di informazioni da parte delle imprese di assicurazioni.

9.5. Marketing

Il settore del *marketing* è stato oggetto di costante attenzione da parte del Garante, in special modo a seguito dei numerosi ricorsi, segnalazioni e reclami relativi ad episodi di ricezione di lettere, telefonate, fax ed altre comunicazioni indesiderate effettuate da operatori del settore.

Una parte cospicua del contenzioso ha riguardato, ad esempio, l'invio di corrispondenza pubblicitaria relativa a proposte di abbonamento a riviste o all'acquisito di alcuni prodotti editoriali.

In proposito, il Garante ha valutato il ricorso di un cittadino che, avendo ricevuto un invito ad abbonarsi ad una rivista pubblicata da una casa editrice italiana (tra l'altro in collaborazione con un editore straniero), non aveva ricevuto riscontro alla richiesta di sapere in che modo la società avesse ottenuto i suoi dati personali, con quali modalità essi venissero utilizzati e per quali scopi. L'Autorità ha pertanto ordinato alla casa editrice di dare completo riscontro alle richieste del ricorrente (*Provv.* 25 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

L'Autorità ha altresì avviato accertamenti nei confronti di una società che offre alcuni servizi aggiuntivi ai clienti che si registrano nel proprio sito *web*. Il Garante, in particolare, intende accertare se gli utenti, al momento della registrazione *on-line*, ricevano un'informativa idonea e se il consenso, che la società chiede di manifestare obbligatoriamente, sia espresso liberamente dagli utenti; ulteriore profilo che l'Autorità intende valutare è se il consenso richiesto faccia riferimento ad un trattamento ben individuato di dati personali o sia, invece, un consenso "*omnibus*" che autorizzi anche l'invio di materiale pubblicitario, vendita diretta, ricerche di mercato o comunicazioni commerciali.

Al vaglio del Garante è altresì la prassi, ormai diffusa fra gli istituti bancari, di raccogliere e trattare dati personali ai fini di *marketing* diretto per la promozione di carte di credito. In merito a tale vicenda l'Autorità ha compiuto accertamenti sulle modalità dei trattamenti effettuati, al fine di verificare la loro conformità al Codice. In particolare, sono state acquisite notizie sull'adempimento degli obblighi di informativa e la raccolta dell'eventuale consenso dell'interessato, nonché sull'origine dei dati personali utilizzati per la promozione delle predette carte.

Al riguardo, tenuto conto della tendenza degli operatori commerciali ad attingere dati personali da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per intraprendere operazioni di *marketing*, il Garante ha ribadito nuovamente, nell'ambito dei menzionati accertamenti, il divieto dell'ulteriore utilizzo per finalità pubblicitarie dei dati estratti dalle liste elettorali, in relazione a quanto previsto dall'art. 177, comma 5 del Codice (che ha modificato l'art. 51 del d.P.R. n. 223/1967). Alla luce di tale quadro legislativo, infatti, le liste elettorali, pur avendo natura di elenchi pubblici, non possono essere più utilizzate da terzi per scopi commerciali o

pubblicitari, a differenza della previgente disciplina che consentiva a chiunque di copiare, stampare o mettere in vendita tali liste.

Con parere del 15 luglio 2004, l'Autorità ha inoltre stabilito che a partire dalla seconda metà del 2005 non potranno più essere adoperati i nominativi contenuti negli elenchi telefonici per realizzare operazioni di *marketing* diretto nei confronti di chi non lo abbia espressamente consentito. Sono state così individuate le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati (ed ai titolari di carte prepagate) negli elenchi cartacei o elettronici disponibili al pubblico, anche con riferimento al diritto dell'interessato di decidere se ricevere o meno pubblicità per corrispondenza o per telefono. Infatti, sarà possibile inviare pubblicità soltanto a chi avrà scelto liberamente, in forma specifica e documentata per iscritto (tramite la compilazione del modello messo a punto dal Garante ed allegato al provvedimento menzionato), di ricevere informazioni commerciali o promozionali; la scelta da parte dell'utente di voler ricevere tali comunicazioni sarà evidenziata da un simbolo associato, a seconda dei casi, all'indirizzo e/o al numero telefonico (cfr. ulteriori considerazioni in merito nel par. 15.3).

L'attività dell'Autorità nella tematica in questione ha riguardato anche l'illecito utilizzo, per finalità pubblicitarie, di fax inviati da altri Stati dell'Unione europea. Grazie ad un sistema di cooperazione tra le istituzioni competenti nei vari stati membri, il quale prevede una procedura di trasmissione delle segnalazioni e dei reclami riguardanti la possibile violazione dell'art. 13 della direttiva 2002/58/CE, è stato possibile intervenire, per il tramite della omologa autorità britannica, anche nei confronti di una società che effettuava dal Regno Unito un invio massivo di fax pubblicitari nel nostro paese.

Infine, nel più ampio contesto dell'autoregolamentazione promossa dall'Autorità, particolare rilevanza riveste per il settore in esame la definizione del codice di deontologia relativo al trattamento dei dati personali a scopo di *marketing* diretto e di invio di materiale pubblicitario, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale. Il codice dovrà tra l'altro prevedere, anche per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale opposizione all'invio di determinate comunicazioni commerciali.

Sono già pervenute all'Autorità alcune richieste di partecipazione ai prossimi lavori preparatori per l'adozione del predetto codice. Il Garante sta valutando tali richieste al fine di individuare i soggetti rappresentativi del settore in esame che prenderanno parte ai lavori.

9.6. *Carte di fidelizzazione*

Già in passato l'Autorità è stata chiamata a pronunciarsi sul tema delle cd. "carte di fedeltà" o tessere di "fidelizzazione" della clientela: si tratta di tessere, spesso rilasciate gratuitamente presso punti di vendita, centri o esercizi commerciali, che consentono ai consumatori di usufruire di sconti o premi. Il rilascio delle predette carte è di regola subordinato alla compilazione di questionari sulle abitudini e le scelte di consumo dei clienti e delle loro famiglie e alla raccolta di ulteriori dati personali in ordine ai volumi di spesa e alle tipologie di prodotti acquistati dal consumatore al fine di consentire alle società titolari del trattamento di compiere operazione di cd. profilazione della clientela. Dalla documentazione acquisita è emerso che spesso gli interessati non hanno una piena consapevolezza di tali operazioni e dei rischi implicati, in quanto non ricevono preventivamente idonee informazioni sulle caratteristi-

che del trattamento dei dati che si accingono a fornire e sugli strumenti posti a difesa dei loro diritti.

L'Autorità ha ritenuto opportuno avviare una consultazione pubblica sul tema volta ad acquisire ulteriori elementi di informazione e documentazione da parte degli operatori dei settori della grande distribuzione e del *marketing*, degli organismi rappresentativi degli operatori dei predetti settori, delle associazioni dei consumatori e di ogni altro soggetto interessato. I quesiti che hanno formato oggetto della consultazione hanno riguardato in particolare: l'individuazione delle prassi seguite in sede di rilascio delle carte, con particolare riferimento alla (necessaria) richiesta del consenso della clientela al trattamento dei dati per la fruizione di benefici di varia natura (premi, sconti o buoni, speditezza e dilazione nei pagamenti ecc.); le modalità e finalità del trattamento dei dati dei clienti e l'individuazione della loro tipologia; gli adempimenti degli obblighi di informativa e consenso; l'eventuale uso in tale ambito delle tecniche di profilazione e classificazione della clientela; i tempi di conservazione delle informazioni raccolte; le misure adottate per agevolare l'esercizio dei diritti degli interessati, nonché l'ambito di comunicazione di tali dati.

9.7. *Flussi transfrontalieri*

Il trasferimento all'estero di dati personali da parte di una società o di una pubblica amministrazione è consentito dalla normativa comunitaria ed italiana solo se il livello di protezione garantito dal Paese di destinazione è adeguato. Si possono, invece, trasferire i dati verso Paesi che non garantiscono tale livello di protezione solo con il consenso degli interessati o sulla base di altri presupposti di liceità indicati all'art. 43 del Codice (esecuzione di obblighi derivanti da un contratto di cui è parte l'interessato, esigenza di salvaguardia della vita e dell'incolumità di un terzo, investigazioni difensive ecc.) oppure con l'autorizzazione del Garante. Al di fuori di questi casi il trasferimento verso Paesi terzi di dati personali è vietato.

Questi principi sono stati ribaditi anche in occasione di una richiesta di intervento urgente del Garante, trasmessa da alcune associazioni a tutela dei diritti dei consumatori, relativamente al trasferimento in Argentina di dati personali di soggetti intestatari di titoli obbligazionari (nell'ambito di una Offerta pubblica di scambio volontaria promossa dalla Repubblica Argentina). Si è precisato, in particolare, che il trasferimento dei dati personali degli investitori che intendono aderire all'offerta della Repubblica Argentina –paese che la Commissione europea ritiene fornisca un adeguato livello di tutela dei dati personali (Decisione 30 giugno 2003, in *G.U.C.E.* 5 luglio 2003)– è lecito solo se necessario per l'esecuzione di obblighi contrattuali o in presenza di uno specifico consenso informato che individui le istituzioni argentine come destinatarie dei dati (art. 43 del Codice).

L'Autorità, a seguito dell'esame della documentazione relativa alla predetta operazione, ha ritenuto che il trasferimento di dati personali degli investitori sia consentito solo in base ai requisiti sopra indicati, fermo restando che i dati, una volta trasferiti, potranno essere poi utilizzati soltanto per le finalità specificate nel rapporto contrattuale (e che potranno essere trasferiti, altresì, solo i dati pertinenti e non eccedenti rispetto a tale rapporto).

Il Garante ha svolto un attento monitoraggio in relazione ad operazioni di "esportazioni" di dati da parte di operatori italiani e al tipo di garanzie e strumenti adottati per tutelare i diritti degli interessati. Nel 2004 è stata portata a conclusione l'indagine (v. *Relazione 2003*, p. 96) presso cinquanta tra le principali società e gruppi industriali che operano in Italia, incentrata sull'analisi dei presupposti, delle

finalità e modalità del trasferimento di dati all'estero, delle categorie di dati trasferiti e delle persone interessate (cittadini, lavoratori, professionisti, imprenditori ed altre società), delle attività dei soggetti importatori, nonché degli strumenti utilizzati per la tutela dei dati personali in rapporto a ciascuna tipologia di trasferimento.

Dall'indagine svolta è emerso che l'oggetto prevalente dei trasferimenti di dati all'estero effettuati dalle società è rappresentato dai dati personali dei dipendenti ed in misura minore, ma sempre rilevante, dalle informazioni relative a clienti, società concorrenti e fornitori. Di regola i flussi di dati sono effettuati dopo aver acquisito lo specifico consenso degli interessati. In alcune limitate ipotesi, quando la gestione delle risorse umane avviene negli Stati Uniti, le società che "importano" i dati personali hanno aderito all'accordo del cosiddetto "*Safe Harbor*". È emersa, inoltre, una diffusa tendenza a predisporre contratti, anche "multilaterali" nel caso di gruppi societari, da sottoporre al parere preventivo del Garante, e a fare uso delle clausole contrattuali *standard* indicate dalla Commissione europea (cfr. *Newsletter* 17 maggio 2004).

Nel corso del 2004 si è assistito, altresì, ad un aumento di richieste di pareri ed informazioni da parte di imprese e gruppi societari, operanti a livello internazionale, in merito alla corretta applicazione della normativa in materia di trasferimento dei dati personali.

In particolare, è attualmente all'esame dell'Autorità una richiesta di parere relativa ad un sistema informativo costituito da una banca dati elettronica e centralizzata –allo stato non più aggiornata, in attesa di verificare appunto la compatibilità del sistema con la normativa sulla protezione dei dati personali– la cui gestione e manutenzione è affidata ad una società che ha sede nel Regno Unito e nella quale confluiscono informazioni trasmesse da istituti di credito, relative a presunte condotte fraudolente tenute da esercenti commerciali convenzionati con un circuito internazionale.

Il *server* che ospita la predetta banca dati è fisicamente collocato al di fuori dell'Ue, in particolare negli Stati Uniti, mentre la consultazione del sistema da parte degli istituti di credito aderenti al circuito avviene su base nazionale.

Da una prima analisi dei quesiti formulati dalla società richiedente, l'Autorità ha potuto rilevare che il trattamento di dati personali effettuato da parte di quest'ultima nell'ambito del sistema descritto potrebbe non essere soggetto alla normativa italiana sulla protezione dei dati personali, trattandosi di un sistema gestito direttamente da un titolare del trattamento stabilito fuori dal territorio dello Stato. In tal caso, infatti, in base al principio di stabilimento previsto dal Codice (art. 5), il trattamento dei dati non ricadrebbe nell'ambito di applicazione della legge italiana. Per quanto riguarda, invece, la trasmissione dei dati al sistema da parte degli istituti bancari italiani, nonché il successivo trasferimento degli stessi al *database* situato negli Usa, il Garante si è riservato di esaminare i profili inerenti la materia di trasferimento dei relativi dati personali all'estero al fine di individuare la disciplina applicabile.

Sempre nel settore dei flussi transfrontalieri di dati riguardanti presunte condotte irregolari connesse all'uso di carte di credito, il Garante ha partecipato attivamente ad un gruppo di lavoro istituito presso il *Working Group* di cui all'art. 29 della direttiva 95/46/CE, insieme a rappresentanti di altre autorità nazionali di protezione dei dati, della Commissione europea, e dell'industria delle carte di credito, con l'obiettivo di individuare alcune linee-guida affinché questi flussi di dati –talvolta limitati all'interno dello spazio comune europeo, talaltra invece su base globale– avvengano nel rispetto dei diritti e delle libertà delle persone interessate. Il documento, in versione non ancora definitiva, è adesso al vaglio del *Working Group* che dovrà tenere conto delle osservazioni formulate in merito da alcune autorità nazionali (tra queste, il Garante).

Sono inoltre giunte all'attenzione dell'Autorità alcune richieste di autorizzazione al trasferimento dei dati all'estero da parte di società di revisione contabile che, in base alla normativa di settore vigente negli Usa (in particolare il recente *Sarbanes-Oxley Act*), per svolgere prestazioni professionali a favore di società quotate nei listini americani sono tenute a registrarsi presso un apposito elenco, detenuto da un organismo americano istituito per monitorare le società che operano nel mercato finanziario. Le società richiedenti hanno infatti evidenziato che, ai fini della relativa registrazione, devono raccogliere e trasmettere all'organismo menzionato informazioni personali relative alle stesse società, ai soci e ai dipendenti, nonché ai consulenti che assistono le società di revisione nello svolgimento dei relativi incarichi. Tali informazioni, peraltro, includono dati giudiziari e fanno altresì riferimento a procedimenti civili, amministrativi e disciplinari o arbitrati in cui sono stati coinvolti i predetti soggetti.

Al riguardo, il Garante sta valutando se siano applicabili al caso descritto i presupposti di liceità richiesti dall'art. 43 del Codice e, più in generale, la compatibilità di tali trattamenti di dati con la normativa italiana e comunitaria.

Con riferimento all'attività svolta dall'Autorità al fine di dare attuazione ad alcune decisioni comunitarie relative al settore in esame, come anticipato nella *Relazione 2003*, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, pubblicata sulla *G.U.C.E.* L 168 del 5 luglio 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina. Va specificato, inoltre, che il 28 aprile 2004 la Commissione europea, con decisione 2004/411/CE, ha stabilito che il livello di protezione dei dati personali esistente nell'Isola di Man, su cui si era già espresso in senso favorevole, con il parere n. 6 del 21 novembre 2003, il Gruppo art. 29, è parimenti "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti. È, infine, in fase di pubblicazione sulla Gazzetta Ufficiale la deliberazione con la quale il Garante ha dato attuazione alla Decisione comunitaria del 21 novembre 2003, n. 2003/821/CE recante il riconoscimento del Baliato del Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

10 Libere professioni

10.1. *Ordini e collegi professionali*

Anche nel corso del 2004 sono pervenuti quesiti sul trattamento dei dati personali relativi a soggetti iscritti ad albi e collegi professionali. Rispondendo ad essi, il Garante ha avuto occasione di ribadire le significative innovazioni introdotte in questa materia dal Codice e di fornire alcune precisazioni in merito alla divulgazione delle informazioni relative a provvedimenti disciplinari.

Al riguardo, si ricorda che, ai sensi dell'art. 61 del Codice, in armonia con le disposizioni sulla comunicazione e diffusione di dati personali da parte dei soggetti pubblici, gli ordini e i collegi professionali possono ora più agevolmente comunicare pure a privati e diffondere, anche mediante reti di comunicazione elettronica, i dati (diversi da quelli sensibili e giudiziari) che, secondo le disposizioni legislative o regolamentari di settore, devono essere necessariamente inseriti nei rispettivi albi per legge o regolamento.

In merito alla divulgazione delle informazioni relative a provvedimenti atti ad incidere sull'attività dell'iscritto all'albo, su richiesta del Consiglio nazionale degli ingegneri, è stato specificato che nelle comunicazioni a soggetti pubblici o privati, o in sede di diffusione, anche per via telematica, di dati inseriti nell'albo professionale, può essere resa nota l'esistenza di provvedimenti disciplinari che dispongono la sospensione dalla professione, ma non il provvedimento nella sua integralità, fermo restando il dovere di porre in circolazione informazioni corrette, complete ed aggiornate, specie con riguardo ad eventuali sviluppi favorevoli per gli interessati.

D'altra parte, in base alla nuova disciplina (art. 61, comma 3, del Codice) gli ordini ed i collegi professionali possono integrare i dati contenuti negli albi con ulteriori informazioni che l'iscritto richieda di aggiungere, purché pertinenti e non eccedenti in relazione alla sua attività professionale (*Nota* 17 agosto 2004).

In risposta ad un quesito di un consiglio notarile distrettuale, l'Ufficio ha poi precisato che, ai sensi dell'art. 61 del Codice, l'esistenza e l'esito del provvedimento di sospensione possono essere comunicati a soggetti privati che abbiano presentato un esposto, ferma restando, peraltro, l'applicazione nel caso concreto delle disposizioni della legge n. 241/1990 in tema di accesso ai documenti amministrativi (*Nota* 17 agosto 2004).

10.2. *Liberi professionisti*

In ossequio ai principi di semplificazione ed efficacia, il Garante, in un articolato parere indirizzato al Consiglio nazionale forense, ha fornito alcuni chiarimenti per una corretta applicazione della disciplina sulla protezione dei dati nell'esercizio dell'attività forense che, per alcuni aspetti, possono valere anche per altri liberi professionisti (*Nota* 3 giugno 2004).

In relazione alla titolarità del trattamento è stato chiarito che, quando l'attività è svolta individualmente, titolare del trattamento è lo stesso avvocato, cui spettano quindi le decisioni sull'uso dei dati, sugli strumenti impiegati e sul profilo della sicu-

rezza, mentre sono contitolari del medesimo trattamento due professionisti che operino congiuntamente. Se l'attività è invece svolta in forma societaria o associata, il titolare è l'entità nel suo complesso e gli adempimenti previsti dal Codice devono essere attuati unitariamente per evitare frammentazioni o ripetizioni da parte dei singoli professionisti. La designazione del responsabile del trattamento è facoltativa e nelle grandi organizzazioni ne possono essere designati anche diversi. Chiunque abbia accesso interno ai dati (praticanti, personale amministrativo ecc.), deve essere designato quale incaricato del trattamento, indicando per iscritto i compiti affidatigli.

Per quanto riguarda gli adempimenti, la maggior parte dei trattamenti effettuati dagli avvocati non sono soggetti a notificazione, mentre resta fermo l'obbligo di informativa all'interessato, che può essere resa anche oralmente e in forma sintetica, purché completa.

Il titolare deve inoltre adottare le misure di sicurezza idonee e preventive per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta. Contrariamente a quanto ipotizzato in alcuni quesiti formulati da singoli professionisti, il Garante ha precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non si deve affatto eliminare il nome delle parti dalla copertina dei fascicoli cartacei. È invece sufficiente seguire adeguate modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

I dati comuni e sensibili possono essere trattati senza il consenso degli interessati solo se il loro uso è necessario per svolgere indagini difensive o far valere un diritto in sede giudiziaria. Se tra i dati sensibili vi sono anche informazioni relative a salute e vita sessuale, è necessario seguire il cd. principio del pari rango, in ragione del quale il diritto difeso o fatto valere in giudizio deve essere un diritto della personalità o un altro diritto o libertà fondamentale o inviolabile (art. 26, comma 4, lett. *c*), del Codice).

Per quanto riguarda il trattamento dei dati giudiziari, purché esso avvenga nel rispetto dell'autorizzazione generale n. 4/2004, non è richiesto il consenso dell'interessato.

L'esercizio dell'attività stragiudiziale (arbitrati, conciliazioni, ricorsi amministrativi) è soggetto, invece, a regole differenti, in base alle quali il trattamento dei dati comuni di soggetti diversi dal cliente deve generalmente avvenire con il consenso dell'interessato, a meno che sia applicabile uno dei presupposti indicati dall'art. 24 del Codice (ad esempio, nel caso di trattamento di dati "pubblici"). Nel caso di dati sensibili, il consenso, sempre necessario, deve essere scritto.

Notai

Nel corso dell'anno, con un parere reso al Consiglio nazionale del notariato, l'Autorità ha precisato le modalità con le quali i notai, in qualità di titolari del trattamento, devono dare applicazione alla normativa in materia di protezione dei dati personali, assumendo un formale impegno a redigere a breve un agevole e sintetico "decalogo", in cooperazione con il Consiglio.

L'Ufficio ha nel frattempo ribadito che la disciplina sulla protezione dei dati personali non pone in discussione la peculiarità della funzione notarile e si affianca alle regole generali sul segreto professionale per assicurare l'integrità e la disponibilità dei dati, indicando come gli stessi debbano essere custoditi e trattati in concreto.

Analogamente a quanto previsto per gli avvocati, il Garante ha chiarito le modalità di applicazione delle misure minime di sicurezza e degli obblighi di informativa all'interessato. Tuttavia, è stato precisato che, data la peculiarità e gli obblighi della funzione notarile, il dare conoscenza o pubblicità ad alcuni dati e documenti trat-

tati dal notaio non concreta la fattispecie della "diffusione" prevista dal Codice.

È stato ricordato, ferme restando le particolari garanzie per i dati sensibili, che il consenso è solo uno dei presupposti del trattamento dei dati comuni: si può, infatti, fare riferimento agli altri presupposti indicati nell'art. 24 del Codice, come, ad esempio, l'adempimento di obblighi di legge o l'esecuzione di obblighi contrattuali (*Nota* 3 dicembre 2004).

11 Rapporto di lavoro e previdenza

11.1. *Dati trattati nel corso del rapporto di lavoro*

Il Garante ha proseguito la valutazione, già iniziata nel 2003, degli effetti delle disposizioni di attuazione della cd. riforma Biagi del mercato del lavoro (l. n. 30/2003 e d.lg. n. 276/2003) con riguardo al trattamento dei dati personali in ambito lavorativo.

L'Autorità, anche con le autorizzazioni generali al trattamento dei dati sensibili, ha ribadito la necessità che il trattamento di taluni dati sensibili sia effettuato nel rispetto delle regole e dei principi generali dettati dal Codice ed entro i limiti fissati dall'art. 8 dello Statuto dei lavoratori (legge 20 maggio 1970, n. 300, che vieta indagini sulle opinioni e trattamenti discriminatori).

La Borsa continua nazionale del lavoro

Il principio è stato altresì indicato in un parere reso il 3 settembre 2004 sullo schema di decreto interministeriale di attuazione della Borsa continua nazionale del lavoro, nel quale il Garante ha sottolineato l'esigenza che il richiamo all'art. 10 del d.lg. n. 276/2003 ivi contenuto sia interpretato in armonia con l'art. 8 della legge n. 300/1970.

Con il citato parere, le cui indicazioni sono state solo in parte recepite nel testo definitivo del decreto del 13 ottobre 2004, sono stati affrontati ulteriori importanti profili in materia di protezione dei dati personali nel sistema della Borsa continua nazionale del lavoro: in particolare, su specifica richiesta dell'Autorità, il regolamento reca ora l'indicazione dei titolari dei trattamenti, al fine di definirne compiutamente le relative responsabilità. Per assicurare il rispetto del principio di proporzionalità del trattamento dei dati, l'indicazione dei dati da far confluire nella Borsa (in particolare, delle informazioni minime ed essenziali relative alle candidature e alle richieste di personale), contenuta negli allegati, è ora esaustiva e si prevede che eventuali ulteriori dati possano essere inseriti solo su base volontaria e non possano essere oggetto, in ogni caso, di utilizzazione a fini discriminatori, specie qualora abbiano natura di dati sensibili, come l'"appartenenza a liste speciali"; è stato altresì precisato nel regolamento che i soggetti che fruiscono della Borsa possono trattare solo i dati pertinenti all'instaurazione del rapporto di lavoro.

Videosorveglianza in ambito lavorativo

Sono stati definiti alcuni procedimenti già istruiti in materia di controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza e sono state fornite prescrizioni ai titolari del trattamento con particolare riferimento al rispetto dell'art. 4 della legge n. 300/1970, oltre che dei principi generali posti dal Codice a garanzia degli interessati.

Il controllo del lavoratore attraverso videocamere è stato oggetto anche di alcuni ricorsi sottoposti al Garante.

I casi affrontati nel corso dell'anno (concernenti impianti di ripresa video installati da soggetti privati) hanno permesso di dare applicazione ai precetti di legge ed alle indicazioni specifiche contenute nel provvedimento generale del Garante del 29 aprile 2004 (v. par. 12.1).

In particolare, nelle decisioni del 16 giugno 2004 e dell'11 ottobre 2004, è stato sottolineato che i trattamenti in questione violavano i presupposti di liceità, propor-

zionalità, correttezza e trasparenza in relazione, tra l'altro, all'angolo di ripresa delle telecamere, all'assenza di idonea informativa o all'invasività dell'impianto stesso di videosorveglianza, nonché alle finalità perseguite che potevano essere raggiunte anche con accorgimenti diversi (nel caso di specie, installazione di cancelli o provvedimenti per regolare gli accessi).

Profili di liceità e correttezza del trattamento in ambito lavorativo

L'Autorità è poi intervenuta su ulteriori temi specifici, tra i quali: adeguatezza della modulistica di informativa e richiesta del consenso dei lavoratori predisposta dai datori di lavoro; accesso dei lavoratori ai dati personali che li riguardano; modalità di conservazione e custodia dei dati dei dipendenti a cura dei datori di lavoro.

È stato esaminato il caso di un dipendente di banca che ha contestato la formula di manifestazione del consenso al trattamento dei dati personali riportati nell'estratto conto certificativo della sua posizione contributiva (cd. "Ecocert") inserita dal datore di lavoro in un modulo con il quale chiedeva all'interessato la delega all'acquisizione di tali dati presso l'ente previdenziale. L'Autorità (*Nota* 7 luglio 2004) ha rilevato che, nel caso di specie, la richiesta del consenso era superflua, in quanto i dati non sensibili erano trattati per adempiere a specifici obblighi fissati dalla normativa vigente (artt. 4 e 24, legge 23 luglio 1991, n. 223) e dagli accordi contrattuali al fine di avvalersi di procedure di riduzione collettiva del personale.

Anche con riferimento agli eventuali dati sensibili contenuti nel modulo "Ecocert", l'acquisizione del consenso dell'interessato è stata ritenuta superflua, dal momento che il segnalante aveva già manifestato alla banca il consenso al trattamento dei dati personali, anche sensibili, per le finalità e nei termini indicati nelle informative già fornite a suo tempo dalla banca e nel cui ambito potevano essere ricomprese anche le operazioni necessarie per adempiere agli obblighi appena richiamati. Si è poi fatto presente che, in base alle nuove disposizioni del Codice, non è più necessario il consenso scritto dell'interessato quando il trattamento dei dati sensibili occorra in rapporto a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro, nel rispetto dell'autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d*), del Codice).

L'Autorità ha pertanto prescritto alla banca di precisare agli interessati, ad integrazione delle informative fornite in passato, che il conferimento dei dati contenuti nel modulo "Ecocert" è necessario per l'adempimento dei predetti obblighi, con l'indicazione delle conseguenze in caso di mancato rilascio di tali dati, e di invitare i lavoratori a produrre direttamente l'estratto conto della propria posizione contributiva in alternativa al rilascio di una delega a tal fine alla banca, tenuto conto che comunque è loro facoltà accedere personalmente ai dati in questione presso gli enti previdenziali (art. 54, legge 9 marzo 1989, n. 88).

Rapporto di lavoro e tutela della dignità e della riservatezza del lavoratore

In numerose ipotesi il Garante è dovuto intervenire a tutela della dignità e della riservatezza dei lavoratori, specialmente se interessati da delicate vicende personali e familiari attinenti allo stato di salute e alla vita sessuale.

Si segnala, al riguardo, l'accoglimento del ricorso della dipendente di una società per una seria violazione della propria riservatezza personale e familiare (*Provv.* 27 luglio 2004, v. *Newsletter* 11-17 ottobre 2004). La dipendente, che occupava temporaneamente la scrivania di un collega, aveva trovato la fotocopia di una lettera da lei stessa inviata al direttore dell'ufficio, nella quale erano riportate anche delicate informazioni sulla condizione di salute della figlia minore disabile.

L'Autorità ha rilevato che la presenza di tale fotocopia contenente dati sensibili

della dipendente e della figlia minore, al di fuori del fascicolo personale e comunque in un contesto inappropriato, contrastava con le prescrizioni e le cautele indicate nell'autorizzazione generale che disciplina il trattamento dei dati sensibili nei rapporti di lavoro, nonchè con le disposizioni del Codice in materia di misure di sicurezza; ha ricordato che i dati sensibili devono essere conservati in una sezione separata del fascicolo personale ed essere accessibili solo al personale autorizzato.

Il Garante, riconosciute le ragioni della dipendente, ha imposto alla società di adottare tutte le misure di sicurezza idonee a prevenire il ripetersi di eventi del genere, comunicandone il contenuto all'Autorità.

La società, che non ha contestato la ricostruzione della vicenda fatta dalla dipendente, ha avviato una indagine interna i cui esiti dovranno essere comunicati al Garante per la valutazione di altre eventuali violazioni o responsabilità.

Cartellini identificativi e mutamento del sesso

L'Autorità ha inoltre affrontato la delicata questione relativa alla possibilità di ottenere la rettificazione degli atti dello stato civile solo a seguito di una sentenza del tribunale passata in giudicato che attribuisca alla persona un sesso diverso da quello enunciato nell'atto di nascita, in ragione delle intervenute modificazioni esteriori dei suoi caratteri sessuali. Tale previsione, pur corrispondendo ad una scelta normativa specifica, che solo il Parlamento ha il potere di modificare, mostra alcuni elementi di criticità in merito alla difesa dei diritti dei soggetti coinvolti nel procedimento di rettificazione del sesso, specie nella fase transitoria di tale procedimento. La lunga durata dei procedimenti di rettificazione di attribuzione di sesso ha reso quindi necessario richiamare l'attenzione sull'esigenza di porre allo studio la possibilità di introdurre nell'ordinamento specifiche misure provvisorie volte a tutelare l'identità personale e la dignità dell'interessato nel periodo preliminare al passaggio in giudicato della sentenza. Spetta al Governo e al Parlamento valutare anche la possibile applicazione di tali misure in eventuali altri procedimenti giudiziari in cui si presentino analoghe esigenze (*Nota* 11 agosto 2004).

Con riferimento all'uso sul luogo di lavoro del nome di battesimo, nell'intervallo di tempo necessario al passaggio in giudicato della sentenza di rettificazione di sesso, l'Autorità ha avuto modo di precisare che, in applicazione dei principi di pertinenza e non eccedenza, sui cartellini identificativi dei dipendenti devono essere presenti unicamente i dati sufficienti ad assicurare la trasparenza dei rapporti tra il personale e tra questi e gli utenti (ad es. l'immagine fotografica, la definizione del ruolo ricoperto ed eventualmente un numero o una sigla) e non anche altri dati non necessari per perseguire tale finalità (es. dati anagrafici). Analogamente, con riferimento alla prassi di indicare il nome di battesimo nell'indirizzo di posta elettronica, nei moduli di richiesta di ferie e/o permessi e nelle comunicazioni personali e domiciliari, l'Autorità ha ricordato che l'interessato che non desidera che su tali atti compaia il suo dato anagrafico non ancora rettificato ha il diritto di richiedere, per motivi legittimi, l'adozione di specifiche misure che, in armonia con la disciplina dettata dal Codice, tengano conto della sua delicata posizione meritevole di tutela (art. 7, comma 4, del Codice). Il datore di lavoro ha l'obbligo di valutarle tempestivamente; l'interessato che ritenga di aver ricevuto una risposta insoddisfacente ha il diritto di adire l'autorità giudiziaria ordinaria o, in alternativa, il Garante con gli strumenti di tutela previsti dal Codice.

Accesso in ambito lavorativo

Diverse ipotesi esaminate hanno avuto origine da richieste da parte del lavoratore di accedere ai dati che lo riguardano detenuti dal datore di lavoro, richieste talvolta estese alla conoscenza di tutte le informazioni utilizzate dallo stesso datore di lavoro in relazione alla carriera professionale dell'interessato (comprese relazioni