

7

Attività giornalistica
e mezzi di informazione

7.1. Tutela dei minori

Nel 2005 sono pervenute varie segnalazioni relative al trattamento di dati effettuato in occasione di servizi giornalistici riguardanti vicende collegate a rapporti o a procedimenti di adozione.

Il Garante ha ricordato che la diffusione di dati idonei ad identificare un minore adottato, oltre a porsi in contrasto con la disciplina sulla protezione dei dati, viola la normativa in materia di adozione nella parte in cui riconosce speciali cautele e procedure per accedere alle relative informazioni, affidando ai genitori la scelta sui modi e i termini per informare il minore della sua condizione (*cf.* *Comunicato stampa* 5 maggio 2005).

Il Garante è anche intervenuto rispetto alla pubblicazione, da parte di un quotidiano locale, di dati che rendevano nel loro insieme identificabili i protagonisti di un caso di adozione; si è evidenziato che le cautele imposte rilevano anche con riferimento a vicende relative ad adottati divenuti maggiorenni (*cf.* *Newsletter* 28 ottobre 2005).

**Dati idonei a rivelare
lo status di adottato**

7.2. Cronache giudiziarie

Hanno trovato ulteriore conferma, nella giurisprudenza nazionale (Tribunale di Milano, sez. I civile, 9 novembre 2004, n. 12746) ed europea (Corte europea dei diritti dell'uomo n. 50774/99, 11 gennaio 2005), i principi affermati nell'ambito di precedenti pronunce del Garante in ordine all'illiceità della diffusione di foto segnaletiche non giustificata da scopi di giustizia e di polizia, anche quando le fotografie vengano mostrate durante conferenze stampa.

Il Garante ha esaminato anche nel 2005 numerose questioni riconducibili al tema della diffusione di dati personali relativi a procedimenti penali. Con particolare riferimento alle cronache su attività di indagine e processuali, l'Autorità, provvedendo nei confronti di una testata giornalistica che aveva pubblicato un'immagine in primo piano di una donna con le manette ai polsi imputata per omicidio, ha ricordato che la diffusione di tali immagini è vietata dalla legge (art. 114, comma 6-*bis*, c.p.p.; art. 8, comma 3, codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, Allegato A.1) del Codice).

All'esito dell'istruttoria di diverse segnalazioni e di alcuni reclami, l'Autorità ha inoltre ribadito che la pubblicazione di dati giudiziari (art. 4, comma, 1, lett. e) del Codice) è ammessa, pur senza il consenso dell'interessato, ma nel presupposto dell'«essenzialità dell'informazione riguardo a fatti di interesse pubblico» (art. 137, comma 3, del Codice, art. 12 del codice di deontologia per l'attività giornalistica) e nella misura in cui i dati non siano relativi ad atti coperti da segreto o non pubblicabili per legge (art. 114 c.p.p.). La sussistenza del carattere di essenzialità dell'informazione deve essere ravvisata necessariamente caso per caso, nel contesto dei fatti narrati (art. 6 codice di deontologia), come già specificato nel documento del 6 maggio 2004 inviato all'Ordine nazionale dei giornalisti (*v.* *Relazione* 2004, pp. 53-54).

**Libertà di informazione
e procedimenti penali**

**Pubblicazione
di fotografie acquisite
in ambito privato**

Alla luce del parametro di essenzialità dell'informazione l'Autorità non ha ravvisato violazioni nella pubblicazione di alcune fotografie a corredo di notizie riguardanti operazioni di arresto (*ad es.*, se tratte da album di famiglia), sul presupposto della loro lecita acquisizione. Una decisione del Garante ha ritenuto legittima la richiesta dell'interessato formulata ad un quotidiano allo scopo di conoscere l'origine di una propria fotografia, pubblicata nel contesto di un articolo che riferiva della richiesta di rinvio a giudizio formulata a carico dell'interessato medesimo (*Provv.* 6 ottobre 2005 [doc. *web* n. 1185330]).

**Diffusione di dati
sulla salute**

Sempre in riferimento alla pubblicazione di fotografie su organi di stampa, l'Autorità ha ritenuto non conforme al canone dell'essenzialità la pubblicazione della foto di un giovane sieropositivo arrestato per alcuni fatti criminosi e successivamente sottoposto ad una diversa indagine per possibili lesioni nei confronti di alcune donne (*Nota* 31 marzo 2005). In tale circostanza è stato ricordato come esistano modalità differenziate, rispettose della dignità e della riservatezza degli interessati, altrettanto idonee ad "allertare", ove necessario, persone che hanno avuto rapporti con soggetti sieropositivi (ad esempio, attivando numeri verdi o altri servizi di informazione e assistenza in grado di fornire opportune informazioni).

**Intercettazioni
telefoniche
e dati di traffico**

Il rispetto del principio di "essenzialità dell'informazione" è stato altresì prescritto dal Garante nella decisione su un reclamo presentato da un noto personaggio che lamentava la diffusione, da parte di organi di stampa, di dati personali contenuti nelle trascrizioni di intercettazioni telefoniche disposte nell'ambito di indagini riguardanti delicati fatti di cronaca (*Provv.* 30 novembre 2005 [doc. *web* n. 1212642]). Il Garante ha ritenuto che l'interesse pubblico connesso alle vicende per le quali era stato instaurato il procedimento penale giustificasse, in termini generali, la possibile diffusione di alcuni dati personali contenuti in atti di indagine depositati ed acquisiti dai giornalisti secondo modalità non risultate allo stato degli atti illecite (in relazione ad atti processuali conoscibili dalle parti).

Tuttavia, non tutte le informazioni diffuse sono risultate necessarie a soddisfare essenziali esigenze di cronaca. È stata perciò ritenuta illecita la diffusione del contenuto di alcune conversazioni telefoniche intercorse tra i reclamanti le quali, diversamente da altre, non presentavano un collegamento, neanche indiretto, con le vicende economico-finanziarie oggetto di cronaca, come pure la pubblicazione del testo di due messaggi *Sms* a contenuto esclusivamente privato e del tutto personale, relativi al rapporto affettivo tra i reclamanti medesimi e che non assumevano alcun rilievo in base al ruolo e alla dimensione pubblica di questi ultimi.

In relazione alla stessa vicenda il Garante ha invece dichiarato inammissibile, per carenza dei necessari presupposti, un ulteriore ricorso presentato in via d'urgenza da uno dei due personaggi coinvolti, che lamentava un pregiudizio imminente ed irreparabile in relazione alla diffusione di notizie, ritenute false, circa la situazione patrimoniale e finanziaria delle aziende del gruppo societario di cui era proprietario.

Eccedente il diritto di cronaca, e quindi illecita, è stata ritenuta anche la riproduzione, a margine di articoli di cronaca sulle indagini relative all'omicidio del vice presidente del Consiglio regionale della Calabria, di parti di documenti recanti dati personali relativi al traffico di utenze telefoniche —compresi alcuni dati accessori e quelli relativi agli intestatari— riportati in una consulenza tecnica disposta nell'ambito di una precedente indagine; siffatta riproduzione aveva infatti comportato la diffusione di dati personali relativi anche a soggetti estranei ai fatti criminosi oggetto di cronaca.

**Conferenza
internazionale
su giustizia
e mezzi di comunicazione**

Il tema dei rapporti "giustizia e media" è stato al centro di una riflessione a livello europeo nell'ambito della 2ª Conferenza europea dei giudici del Consiglio d'Europa (Cracovia, 25 e 26 aprile 2005) le cui conclusioni (consultabili all'indirizzo *web* www.coe.int, unitamente al rapporto della delegazione italiana) evidenziano la neces-

sità di adottare misure che concilino le diverse esigenze di trasparenza della giustizia e di libero convincimento dei giudici, con la tutela della dignità umana, della *privacy*, della reputazione e con la garanzia della presunzione di innocenza.

Vari ricorsi, segnalazioni e reclami pervenuti nel periodo di riferimento hanno riguardato la pubblicazione di dati personali relativi a vittime di episodi criminosi.

Il Garante ha in primo luogo ricordato l'esistenza di limiti precisi dettati dalla legge in relazione a crimini specifici, ad esempio a tutela delle vittime di reati sessuali (art. 734-*bis* c.p.); ha conseguentemente vietato ad un settimanale di pubblicare i dati identificativi di una giovane donna vittima di un tentativo di violenza (*Prov. 13 luglio 2005 [doc. web n. 1152088]*).

Rispondendo ad alcune segnalazioni e richieste di parere, l'Autorità ha poi segnalato che, anche fuori dei casi in cui sussistano specifici limiti di legge, i mezzi di informazione sono tenuti pur sempre ad osservare un particolare rigore nel valutare l'essenzialità dell'informazione rispetto a fatti di cronaca e nel fare riferimento alle vittime di azioni delittuose (furti, rapine, aggressioni, ecc.).

All'attenzione dell'Autorità sono pervenuti anche diversi articoli, relativi soprattutto alla cronaca locale, che riferivano di decessi avvenuti in contesti o per cause particolari (uso di sostanze stupefacenti, malori, incidenti). In alcuni casi è stata riscontrata la violazione del limite di "essenzialità dell'informazione", come nel caso della pubblicazione di dati personali relativi alla sfera personale del deceduto e di quella dei suoi familiari, risultati eccedenti e non pertinenti rispetto all'evento narrato, ovvero in relazione alla pubblicazione di articoli contenenti descrizioni particolarmente impressionanti del delitto (art. 8, comma 1, codice di deontologia). L'Autorità ha altresì ricordato che, in simili del genere, i diritti di cui all'art. 7 del Codice possono essere esercitati legittimamente dai familiari del deceduto, anche in riferimento ai dati personali dello stesso, mentre eventuali azioni di risarcimento dei danni restano esercitabili, ove ne ricorrano i presupposti, solo dinanzi all'autorità giudiziaria ordinaria (*Prov. 21 dicembre 2005 [doc. web n. 1217538]*).

Infine, in occasione del decesso di un personaggio noto nell'ambiente sportivo, avvenuto nel corso di una diretta televisiva, il Garante, nell'immediatezza del fatto, ha allertato i mezzi di informazione affinché si astenessero dal pubblicare foto o dal mandare in onda filmati lesivi della dignità e della riservatezza dell'interessato. L'Autorità ha poi dato atto che gli stessi mezzi di informazione si erano autonomamente attenuti a tali cautele, essendosi limitati a diffondere immagini con inquadrature a distanza (*Comunicati stampa 4 ottobre e 18 novembre 2005*).

Il tema dell'informazione in connessione con lo sviluppo tecnologico è rimasto d'attualità anche in relazione a vicende terroristiche e all'uso del *web* per divulgare messaggi ed attività eversive. L'Assemblea parlamentare del Consiglio d'Europa ha sollecitato l'elaborazione di un codice di condotta per i giornalisti ed ha chiesto ai professionisti del settore di "astenersi dal pubblicare immagini scioccanti di atti terroristici che violano la *privacy* e la dignità delle vittime" (Raccomandazione 1706(2005) del 20 giugno 2005).

7.3. Dati idonei a rivelare lo stato di salute

È stato esaminato un caso significativo in relazione al servizio di cronaca pubblicato da un quotidiano a tiratura nazionale, incentrato sulla vicenda di una donna, in coma irreversibile e in stato di gravidanza, e sulla decisione dei medici e dei familiari di tenerla se necessario in vita artificialmente per consentire la nascita prematura di un figlio.

**Vittime di reati
e resoconti sui decessi**

**Atti terroristici
e deontologia
del giornalista**

**Pubblicazione
di dati sulla salute
e dignità della persona**

Il Garante ha ritenuto illecito il servizio che aveva portato a pubblicare dati non indispensabili che nel loro insieme avevano reso identificabili gli interessati, specie nel loro contesto territoriale, fornendo informazioni di natura strettamente clinica relative alla donna, nonché a possibili convinzioni etico-religiose dei suoi familiari (in violazione degli artt. 5 e 10 del codice di deontologia). Il Garante ha stigmatizzato, altresì, il comportamento tenuto dalla struttura sanitaria dalla quale erano evidentemente state attinte tali informazioni, rilevando che, in assenza di un preciso consenso da parte dei familiari a siffatta comunicazione, i sanitari avrebbero dovuto attenersi al rispetto del segreto professionale (*Prov. 13 luglio 2005 [doc. web n. 1152080]*).

È stata riscontrata un'altra grave violazione in riferimento alle modalità con le quali alcune testate giornalistiche, anche attraverso il proprio sito *web*, hanno diffuso informazioni concernenti una persona in condizioni di salute particolarmente critiche (indicata, a seconda delle testate, mediante le generalità o altri riferimenti idonei a renderla agevolmente identificabile), con specifici riferimenti anche ai sintomi della patologia e alle ipotesi formulate sulla diagnosi (sindrome di Creutzfeldt-Jakob e sue varianti, comunemente note come morbo della "mucca pazza"). Come già avvenuto in passato in un caso analogo (*Relazione 2002*, p. 95), il Garante ha precisato che la circostanza che l'illecita pubblicazione trovasse origine in notizie diramate da talune agenzie di stampa —le quali non avevano ommesso di indicare le generalità dell'interessato— non esimeva comunque altre testate giornalistiche dal dovere di garantire l'anonimato dell'interessato (*Prov. 23 novembre 2005 [doc. web n. 1225898]*).

Si è poi concluso il procedimento relativo ad un servizio trasmesso da un'emittente televisiva e concernente un soggetto "senza fissa dimora" (*Prov. 7 luglio 2005 [doc. web n. 1170284]*). Dopo un temporaneo provvedimento di blocco (*v. Relazione 2004*, p. 55) il Garante ha vietato all'emittente di diffondere alcune immagini che mostravano l'interessato in un evidente stato di difficoltà fisica e psichica, ritenendole lesive della sua dignità, oltre che raccolte in violazione dei principi di correttezza e di trasparenza (art. 11, comma 1, lett. *a*) del Codice; art. 2 del menzionato codice di deontologia).

7.4. Libertà di informazione e personaggi pubblici

Rispetto alle persone note, o che esercitano funzioni pubbliche, il giornalista dispone di margini più ampi nella diffusione di informazioni personali ove queste assumano rilievo in base al ruolo o al carattere pubblico dell'attività dei soggetti interessati (*cf. anche Relazione 2004*, p. 55). Il principio è stato ribadito dall'Ufficio del Garante nel rispondere a diverse segnalazioni pervenute nel corso dell'anno, inoltrate da esponenti del mondo politico, di quello giornalistico e dello spettacolo (*Provvedimenti 7 luglio 2005 [doc. web n. 1170291 e n. 1170297]*).

Il rilievo pubblico di una persona non può affievolire la tutela riconosciuta a congiunti e, in particolare, ai minori. Il principio è stato riaffermato dal Garante nel riconoscere la fondatezza di una segnalazione e di un reclamo con cui si lamentava l'illiceità della pubblicazione delle generalità di minori e di altri soggetti nel contesto di articoli incentrati su vicende riguardanti esponenti politici locali.

L'Autorità è poi intervenuta nei confronti di un settimanale che, nel dare notizia di un presunto legame sentimentale di un noto personaggio, aveva pubblicato un articolato servizio fotografico in cui comparivano componenti della sua famiglia ritratti in alcuni momenti di vita privata. In particolare, oltre alle immagini della

moglie, della suocera e dei figli —dei quali almeno uno risultava riconoscibile, poiché il suo volto era stato solo parzialmente oscurato—, il settimanale aveva pubblicato diversi altri dati personali, unitamente alle foto del luogo di residenza e della palazzina di famiglia. Sulla questione pende un contenzioso dinanzi all'autorità giudiziaria ordinaria, essendosi impugnato il provvedimento con cui il Garante ha vietato la pubblicazione di tali fotografie (art. 152 del Codice) (*Provv.* 23 novembre 2005 [doc. *web* n. 1200112]).

Si è ritenuto che concretizzassero una violazione dei limiti del diritto di critica e di cronaca anche i riferimenti personali contenuti in un ampio servizio giornalistico pubblicato da un giornale locale, concernente la denuncia di un possibile giro di usura nell'ambito di alcune case da gioco. Secondo il Garante, la diffusione di diversi dati personali relativi all'autore della denuncia —presidente di un'associazione, conosciuto anche per le sue prese di posizione pubbliche— aveva violato il principio di essenzialità dell'informazione che comporta anche il dovere del giornalista di evitare riferimenti a congiunti o ad altri soggetti non interessati ai fatti riportati (art. 5, comma 1, codice di deontologia; *Provv.* 7 luglio 2005 [doc. *web* n. 1170311]).

A seguito della segnalazione di un giornalista che opera per Rai-Radio televisione italiana S.p.A., l'Ufficio del Garante ha poi ribadito l'orientamento dell'Autorità in ordine alla conoscibilità di classi stipendiali, indennità ed altri emolumenti corrisposti ad amministratori, dirigenti e lavoratori dipendenti ed autonomi da concessionari di pubblici servizi, atteso anche l'interesse pubblico ad ottenere notizie sulle prassi in atto presso tali enti e sull'utilizzo delle relative risorse.

Non è stato invece ravvisato un analogo interesse in riferimento alla pubblicazione dell'indirizzo completo dell'abitazione privata di una giornalista, diffuso nella rubrica di posta di una rivista in risposta alla richiesta di una lettrice. Nel fornire riscontro alla segnalazione, l'Ufficio del Garante ha rilevato che la finalità informativa perseguita dal settimanale poteva essere soddisfatta senza diffondere tale informazione, fornendo semmai una risposta diretta e privata alla sola lettrice interessata.

In relazione ai ripetuti servizi giornalistici dedicati al grave malore e al ricovero di un noto imprenditore per cause legate all'abuso di sostanze stupefacenti, il Garante ha poi ricordato che, anche quando si tratti di figure pubbliche, stampa e media devono rispettare la dignità delle persone e la loro sfera più intima, astenendosi dal diffondere dettagli non indispensabili ed evitando spettacolarizzazioni e accanimenti morbosi; ha quindi ritenuto illecita —e vietato— la pubblicazione di alcuni dettagli eccedenti, idonei a rivelare possibili abitudini sessuali dell'interessato (*Provv.* 12 gennaio 2006 [doc. *web* n.1213631]). Anche questo provvedimento è stato impugnato, da una delle testate interessate.

7.5. *Esercizio dei diritti e diritto all'oblio*

Concludendo la relativa istruttoria, il Garante ha ritenuto illecita la nuova diffusione, nel corso di una trasmissione televisiva, delle immagini di un processo —già mandate in onda sedici anni prima—, che ritraevano una donna mentre reagiva vivacemente alla richiesta di condanna, formulata dal pubblico ministero nei confronti di persona a cui la stessa era all'epoca legata sentimentalmente. L'Autorità ha ravvisato in questo caso la necessità l'esigenza di garantire il diritto all'oblio e all'identità personale; ha infatti rilevato che le immagini erano state riproposte senza tenere in debito conto il diritto dell'interessata a veder rispettata la propria attuale dimensione sociale e affettiva, ed erano state diffuse anche in vio-

**Dati personali
contenuti in denunce
e atti pubblici**

**Diritto all'oblio, tutela
dell'identità personale
e informazione on-line**

lazione del principio dell'essenzialità dell'informazione (*Provv.* 7 luglio 2005 [doc. *web* n. 1148642]).

Garantire un'effettiva tutela del "diritto all'oblio" risulta più difficile nel caso di notizie diffuse attraverso siti Internet. Il Garante ha affrontato al riguardo il caso di una donna che si era rivolta ad un quotidiano per rendere anonima la notizia, contenuta in un articolo pubblicato nel 2002 e ancora presente sul sito *web*, relativa al suo arresto e al successivo rinvio a giudizio, disposti in relazione ad un reato per il quale era stata assolta. Accogliendo tale richiesta l'editore aveva sostituito le generalità della donna con una più generica locuzione ("nota immobiliare milanese"); ha tuttavia precisato che la permanenza in Internet dell'articolo in forma non "anonimizzata" era dovuta alla sua pregressa indicizzazione attraverso alcuni motori di ricerca, e che l'articolo doveva pertanto ritenersi tratto non dagli archivi dell'editore, ma da altri basi dati desunte tramite motori di ricerca (*Provv.* 9 novembre 2005 [doc. *web* n. 1200127]; sul tema dei motori di ricerca, si vedano anche i parr. 2.11 e 15.11).

8 Associazioni, movimenti politici e partiti

8.1. Associazioni

Sono pervenute all'Autorità nuove segnalazioni e richieste di chiarimenti in ordine alle modalità con cui istituti di patronato e di assistenza sociale raccolgono dati relativi a lavoratori, pensionati, disabili ed altri soggetti aventi diritto a prestazioni in materia di previdenza, assistenza sociale e sanitaria per finalità informative e promozionali. In particolare è emerso che le strutture sanitarie competenti per accertare l'invalidità civile trasmettono regolarmente all'Associazione nazionale mutilati e invalidi civili (Anmic) elenchi nominativi di coloro che fanno istanza per il riconoscimento dell'invalidità, o richiedono a tali persone di manifestare il loro consenso alla trasmissione dei dati che li riguardano. Queste informazioni verrebbero successivamente utilizzate dall'Anmic per sollecitare agli interessati l'adesione all'associazione, senza che ne sia peraltro chiarito il carattere facoltativo.

L'Autorità — che era già intervenuta sull'argomento con precisi rilievi sull'ammissibilità della trasmissione di elenchi nominativi di disabili all'Anmic, ad altri patronati e ad associazioni assistenziali e di categoria, fatto salvo l'accesso di tali organismi ai dati anche sensibili degli interessati che abbiano conferito una specifica delega: *cfr., ad es., Nota* 17 settembre 1997 [doc. *web* n. 1055114] — ha avviato ulteriori accertamenti per verificare il rispetto delle disposizioni in materia di trattamento dei dati personali, anche in relazione al nuovo assetto normativo previsto dalla l. 30 marzo 2001, n. 152 (recante “Nuova disciplina per gli istituti di patronato e di assistenza sociale”) e dal Codice.

**Istituti di patronato
e di assistenza sociale**

8.2. Movimenti politici e propaganda elettorale

Con riferimento alle attività di partiti e di movimenti politici, il Garante è stato chiamato più volte ad individuare un punto di equilibrio tra iniziative intraprese a fini di propaganda elettorale da tali organismi (inclusi comitati promotori, di sostenitori e singoli candidati), tenendo presente che simili iniziative costituiscono un momento significativo della partecipazione alla vita democratica (art. 49 Cost.) che richiede comunque un'adeguata protezione dei diritti e delle libertà fondamentali delle persone cui si riferiscono informazioni personali utilizzate (art. 2 del Codice).

L'Autorità ha fornito nuovi chiarimenti di ordine generale, anche nel caso segnalato da un cittadino il quale lamentava che, in diversi seggi di un comune durante le consultazioni elettorali del 12 e 13 giugno 2004, i rappresentanti dei gruppi dei candidati presso la sezione detenevano le liste sezionali degli elettori sulle quali venivano riportate le generalità dei cittadini che esercitavano il diritto di voto (*Nota* 24 febbraio 2005).

A tal proposito sono stati richiamati principi già evidenziati nel *provvedimento* generale del 12 febbraio 2004 (*cd. “decalogo elettorale”* [doc. *web* n. 634369]), con cui erano stati individuati, fra l'altro, limiti e prescrizioni per il trattamento di dati personali anche da parte di scrutatori e rappresentanti di lista. Nella medesima cir-

**Interventi
in materia di elezioni
e consultazioni politiche**

costanza è stato precisato che, in occasione di consultazioni elettorali e di referendum, nonché in sede di verifica della loro regolarità, risulta possibile, in conformità alla legge, raccogliere alcuni dati sensibili degli elettori, in quanto il Codice considera di rilevante interesse pubblico il trattamento di tale categoria di dati per applicare la disciplina in materia di elettorato attivo, passivo e per esperire specifici compiti concernenti, in particolare lo svolgimento di consultazioni elettorali, le richieste di referendum e la verifica delle relative regolarità (artt. 20, 22 e 65). L'Ufficio del Garante ha tuttavia ribadito che scrutatori e rappresentanti di lista, nell'esercizio dei compiti loro affidati o riconosciuti dalla legge, devono osservare particolari cautele in tema di riservatezza in relazione ai dati personali anche di natura sensibile di cui vengono lecitamente a conoscenza. I dati devono essere trattati con ogni opportuna cautela, anche a tutela del principio costituzionale della libertà e segretezza del voto, tanto più in quelle ipotesi (quali referendum abrogativi, o votazioni di ballottaggio) nelle quali l'avvenuta o mancata partecipazione alle operazioni di voto può evidenziare, di per sé, anche una particolare opzione politica dell'elettore. È stata quindi ritenuta illecita la compilazione, effettuata da scrutatori e rappresentanti di lista di elenchi di persone astenutesi dalla partecipazione al voto, ai fini di un successivo utilizzo a fini politici da parte della persona che li ha raccolti o della formazione politica di riferimento (*ad es.*, allo scopo di sollecitare gli elettori rispetto a futuri appuntamenti elettorali).

L'Autorità è intervenuta in materia anche con un provvedimento generale in materia di comunicazioni e di propaganda politica, adottato in previsione sia delle elezioni amministrative di aprile e maggio 2005, sia delle consultazioni referendarie tenutesi nel giugno del medesimo anno (*Prov. 3 marzo 2005* [doc. web n. 1107658], in *G.U.* 18 marzo 2005, n. 64). Con tale provvedimento, nel confermare le prescrizioni del citato "decalogo elettorale" del 12 febbraio 2004, il Garante ha di nuovo evidenziato i casi in cui, in vista delle consultazioni elettorali, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono utilizzare dati personali a fini di propaganda politica senza chiedere preventivamente agli interessati uno specifico consenso.

L'Ufficio del Garante ha poi curato l'applicazione di questi principi chiarendo, tra l'altro, ad un cittadino —il quale lamentava la ricezione di messaggi di propaganda elettorale sulla base dell'utilizzo di dati personali ritenuti coincidenti con quelli detenuti presso gli uffici anagrafici e l'ufficio elettorale di un comune— che risulta possibile utilizzare dati personali senza il consenso degli interessati a fini di propaganda elettorale, solo quando i dati siano estratti da fonti "pubbliche" nel senso proprio del termine e siano quindi conoscibili da chiunque senza limitazioni; ciò, fermo restando il diritto dell'interessato di rivolgersi direttamente al candidato che invia messaggi di comunicazione politica, al fine di esercitare i diritti di cui all'art. 7 del Codice e di ottenere l'aggiornamento, la rettificazione, l'integrazione o la cancellazione dei dati (artt. 7, 8, 9 e 10 del Codice) (*Nota 2 agosto 2005*).

I medesimi principi sono stati in seguito applicati rispetto alla segnalazione di un cittadino che lamentava di non aver ricevuto riscontro alla richiesta di accesso ai dati personali rivolta ad una coalizione politica che gli aveva inviato messaggi di propaganda elettorale (*Nota 17 gennaio 2006*). Nella circostanza si è anche ricordato all'interessato che in caso di mancato riscontro da parte del titolare del trattamento può ricorrersi all'autorità giudiziaria o al Garante (art. 145 del Codice).

In questo quadro è stata trattata anche una segnalazione che lamentava una violazione in materia di trattamento dei dati personali riguardo all'invio di messaggi di propaganda elettorale in occasione delle consultazioni elettorali del 3 e 4 aprile 2005, inviati ad un minore da un candidato che ne avrebbe ottenuto il nominativo

dall'ufficio anagrafe di un comune, in qualità di componente del consiglio comunale (Nota 3 agosto 2005).

In vista delle consultazioni politiche del 9 e 10 aprile 2006, il Garante è da ultimo intervenuto con un nuovo provvedimento generale sulla propaganda elettorale per chiarire le modalità per utilizzare lecitamente i dati personali dei cittadini (*ad es.*, indirizzo, telefono, *e-mail* ecc.) (Prov. 7 settembre 2005 [doc. web n. 1165613], in *G.U.* 12 settembre 2005, n. 212). Con il nuovo intervento si è inteso richiamare nuovamente l'attenzione di partiti, organismi politici, comitati promotori e singoli candidati, in termini agevolmente comprensibili ed applicabili, sulle indicazioni a suo tempo fornite nei citati provvedimenti del febbraio 2004 e del marzo 2005. Si è potuto così estenderne l'ambito di applicazione alle selezioni dei candidati effettuate tramite consultazioni primarie.

Il provvedimento ha nuovamente individuato i casi nei quali può non richiedersi il consenso degli elettori per inviare materiale di propaganda. In particolare, si è confermato il principio in base al quale il consenso non è necessario quando si usano dati personali contenuti nelle liste elettorali detenute dai comuni, dati di iscritti ed aderenti a partiti e organismi politici o dati degli abbonati presenti nei nuovi elenchi telefonici accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere, rispettivamente, corrispondenza a domicilio o chiamate telefoniche. L'Autorità ha anche evidenziato che il consenso è invece necessario per particolari modalità di comunicazione elettronica come *Sms*, *Mms*, *e-mail*, oltre che per telefonate preregistrate e fax. Sono stati ribaditi, infine, i casi nei quali i cittadini devono essere informati sull'uso delle informazioni personali che li riguardano, anche tramite modalità semplificate (art. 13 del Codice), nonché sui diritti che possono essere esercitati ai sensi dell'art. 7 del Codice.

Va rilevato, a conferma della particolare delicatezza dell'utilizzo dei dati personali in tali contesti, che i principi in questione hanno continuato ad essere oggetto di varie richieste di chiarimenti all'Ufficio del Garante, anche dopo l'adozione del nuovo "decalogo" (*v. Nota 4 novembre 2005*).

Sempre rispetto alla tematica in esame, va evidenziata una delicata fattispecie all'esame dell'Autorità che riguarda le richieste di rilascio di copia delle liste elettorali rivolte ai comuni da società specializzate in servizi per il *marketing* diretto, le quali intendevano utilizzare le informazioni ivi contenute al fine di effettuare, per conto di propri clienti ed attraverso specifiche banche dati, campagne di propaganda elettorale e di carattere socio-assistenziale, nonché per perseguire interessi collettivi o diffusi.

In tale ambito si è già correttamente pronunciato il Ministero dell'interno, Dipartimento per gli affari interni e territoriali-Direzione centrale dei servizi elettorali, evidenziando che le liste elettorali non possono essere rilasciate in copia a chiunque, potendo essere comunicate solo *"per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso"* (art. 177, comma 5 del Codice, che ha in parte modificato l'art. 51 d.P.R. 20 marzo 1967, n. 223). Il Ministero ha quindi constatato che le finalità che legittimano il rilascio di copia delle liste elettorali, oltre che essere motivate ai sensi di tale art. 51, devono essere riferibili a scopi perseguiti direttamente dal richiedente e, ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività stessa di tale organismo. Pertanto, sempre secondo il Ministero, richieste come quelle in questione non possono essere accolte anche quando le società dichiarino — come nel caso di specie — di annoverare tra i propri clienti soggetti aventi titolo a richiedere le liste elettorali, anche perché l'oggetto dell'attività imprendito-

**Utilizzo delle liste
elettorali per finalità
di marketing**

riale esercitata non esclude la possibilità di un utilizzo dei dati personali contenuti nelle liste elettorali per finalità anche diverse ed ulteriori rispetto quelle di cui al predetto art. 51 d.P.R. n. 223/1967.

Albo degli scrutatori

Ulteriori elementi di approfondimento sono stati rappresentati da una prefettura con riferimento alla liceità del rilascio, da parte dei comuni, di una copia degli albi degli scrutatori di seggio elettorale a partiti politici. L'Ufficio del Garante ha ricordato che la comunicazione di dati personali a privati da parte di un soggetto pubblico è ammessa unicamente quando prevista da norme di legge o di regolamento (art. 19, comma 3, del Codice). Si è così evidenziato che la normativa di riferimento stabilisce che l'albo degli scrutatori debba restare depositato in un periodo determinato, durante il quale ogni cittadino del comune ha diritto di prenderne visione (art. 3, comma 4, l. 8 marzo 1989, n. 95), salve eventuali altre specifiche disposizioni in materia elettorale che prevedano espressamente una comunicazione o permettano, in modo parimenti espresso, di accedere ad altri elenchi in materia, quali ad esempio quelli relativi agli scrutatori nominati dalla commissione elettorale comunale (art. 6 l. n. 95/1989) (*Nota* 28 marzo 2006).

Voto degli italiani all'estero

In materia elettorale l'Autorità è stata interpellata anche dalla Direzione generale per gli italiani all'estero e le politiche migratorie del Ministero degli affari esteri. La Direzione, inoltrando un quesito formulato dal Consolato generale di Francoforte, ha chiesto di conoscere se era possibile estendere il regime di conoscibilità dell'elenco provvisorio dei residenti all'estero aventi diritto al voto, in riferimento a finalità di carattere politico-elettorale connesse a consultazioni comunali in Germania per le quali anche i cittadini italiani ivi residenti godono dei diritti di elettorato attivo e passivo. L'Ufficio ha evidenziato che tale elenco provvisorio è soggetto a un particolare regime di conoscibilità, espressamente vincolato dalla disciplina di riferimento al perseguimento di specifiche finalità. Poiché le limitazioni al relativo utilizzo non derivano dalla normativa in materia di protezione dei dati personali, si è rappresentata al Ministero l'opportunità di valutare se la finalità di carattere politico-elettorale in questione possa essere perseguita mediante l'applicazione di altre diverse disposizioni di settore in vigore (*Nota* 3 marzo 2006).

Documento comune delle autorità di protezione dei dati

In materia di propaganda elettorale occorre, infine, richiamare le conclusioni cui sono giunti i rappresentanti delle autorità di protezione dei dati personali europee e non, riunite in occasione della 27^{ma} Conferenza internazionale sulla protezione dei dati (Montreux -Svizzera-, 14-16 settembre 2005). Su iniziativa dell'Autorità italiana è stata adottata una risoluzione relativa all'utilizzo di dati personali per la comunicazione politica, che ha trovato il sostegno dell'autorità federale svizzera per la protezione dei dati, dell'autorità federale tedesca per la protezione dei dati, dell'Ispettore generale per la protezione dei dati della Polonia e del Commissario per la protezione dei dati della città di Berlino. Si è così evidenziata, in particolare, la necessità di raccogliere e di utilizzare solo dati indispensabili, di informare i cittadini su chi tratta i dati e sull'uso che ne viene fatto, di ottenere, nei casi previsti, il consenso degli interessati quando si usano particolari forme di comunicazione (come messaggi *Sms* o *e-mail*), di raccogliere le informazioni da fonti lecitamente accessibili e di utilizzare i dati solo a fini di propaganda elettorale (*cfr.*, *amplius*, il par. 22).

9

Attività economiche

9.1. *Credito*

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.

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.

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

**Accesso ai dati
personali e accesso
alla documentazione
bancaria**

**Rimessa interbancaria
diretta**

**Trattamenti effettuati
nell'ambito dei sistemi
di rilevazione creditizia**

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).

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

Contributo-spese
per l'accesso ai dati Sic

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.

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 (*cf.*, 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 ; *cf.* 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-

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

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.

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) (*Prov. 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 rinvienga 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

Identificazione
della clientela
presso istituti bancari
e postali

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 (*cf.* 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

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 (*Prov. 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

DOCUMENTI E RELAZIONI

**Accesso
agli atti assicurativi
e protezione dei dati**

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).

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 (*cf. 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