Accesso ai dati conservati nel C.e.d.

Il Codice ha ulteriormente valorizzato le garanzie per l'interessato in materia di accesso ai dati personali che lo riguardano, in riferimento alla circostanza che la disciplina vigente per l'accesso ai dati conservati nel C.e.d. si applica anche ai dati comunque trattati da organi o uffici di polizia con l'ausilio di strumenti elettronici, nonché a quelli –già espressamente considerati in passato– destinati a confluire nel C.e.d. medesimo (art. 10, commi 3, 4 e 5, l. n. 121/1981 e art. 56 del Codice).

A fronte dell'accresciuto quadro di garanzie, il Garante, nell'esaminare alcune segnalazioni pervenute, ha non di rado constatato l'inadeguatezza del riscontro fornito dal competente ufficio della pubblica sicurezza alle richieste di accesso, di rettifica o di cancellazione dei dati registrati nel C.e.d. presentate dall'interessato.

In alcuni casi, infatti, contrariamente a quanto chiaramente previsto dallo stesso art. 10 della l. n. 121/1981, l'ufficio competente non ha fornito all'interessato la "comunicazione in forma intellegibile" dei dati registrati nel C.e.d.; in altri, la richiesta di modifica o di cancellazione dei dati, benché supportata da documentati esiti processuali, è stata riscontrata con la sola, generica comunicazione che la posizione dell'interessato nella banca di dati risultava aggiornata o che erano state apportate le richieste modifiche ai dati. L'Autorità intende avviare un ciclo generale di accertamenti e verifiche presso gli archivi del C.e.d. tenendo conto del numero ingente di casi per i quali il riscontro fornito dal Dipartimento non è risultato soddisfacente, al fine di verificare l'effettiva corrispondenza delle operazioni compiute dal Dipartimento della pubblica sicurezza alle richieste di rettifica o di cancellazione dei dati presentate dagli interessati e, più in generale, affinché i trattamenti effettuati nell'ambito del C.e.d. si svolgano nel tempestivo e sostanziale rispetto delle garanzie previste dal Codice.

Particolari tecnologie

Sempre nel quadro delle più ampie garanzie previste dal Codice, deve essere prestata particolare attenzione a taluni trattamenti effettuati per finalità di polizia che presentano maggiori rischi per l'interessato in quanto riferiti a dati genetici, biometrici o effettuati mediante tecniche basate su dati relativi all'ubicazione.

Per tali trattamenti l'Autorità intende prescrivere, anche su comunicazione degli organi interessati, particolari misure ed accorgimenti a garanzia dell'interessato (artt. 55 e 17, del Codice) ed ha già segnalato la necessità di individuare tali misure in relazione alla raccolta dei rilievi dattiloscopici effettuata in occasione del rilascio o del rinnovo del permesso di soggiorno agli stranieri e all'eventuale inserimento dei dati biometrici nel documento di soggiorno elettronico.

6.2. *Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza*

Il Garante ha svolto anche nel periodo di riferimento l'attività di verifica su specifici trattamenti di dati personali effettuati presso gli organismi competenti in materia di informazioni e di sicurezza (SISMI, SISDE e CESIS), disciplinati ora dall'art. 58 del Codice.

Questa disposizione, oltre a specificare quali regole del Codice sono applicabili a tali trattamenti, stabilisce che, con decreto del Presidente del Consiglio, si provveda ad individuare le misure minime di sicurezza e le modalità di applicazione a tali trattamenti delle pertinenti disposizioni del Codice. La previsione di tali decreti assume particolare importanza per assicurare, anche in sintonia con orientamenti giurisprudenziali internazionali in materia di tutela dei diritti dell'uomo, trasparenza ai trattamenti effettuati per tali finalità, in relazione ai tipi di operazioni e di dati trattati, l'aggiornamento e la corretta conservazione dei dati mede-

simi. L'Autorità si accinge quindi a prestare la propria collaborazione a partire dai profili relativi alle misure di sicurezza.

Il Garante ha effettuato gli accertamenti rispetto alle segnalazioni presentate dai soggetti interessati, in conformità a quanto previsto dal Codice (art. 160) e con le modalità già osservate nel corso dei precedenti anni.

I controlli, che hanno fatto seguito a quelli effettuati nel marzo 2003, sono stati concentrati nel quinto gruppo di verifiche effettuate dal Garante a decorrere dalla sua istituzione (per un totale di circa 40 persone che hanno chiesto accertamenti) e si sono svolti con la piena collaborazione dei predetti organismi, permettendo di fornire un riscontro dell'attività svolta agli interessati nei particolari termini previsti dal Codice all'esito degli accertamenti.

6.3. *Il controllo sul Sistema di informazione Schengen*

Il Codice ha introdotto importanti modifiche alle modalità di esercizio del diritto di accesso al Sistema di informazione Schengen (SIS) e degli altri diritti connessi (rettifica, integrazione o cancellazione), che possono ora essere esercitati direttamente nei confronti dell'autorità di polizia (c.d. accesso "diretto") e non più solo "per il tramite" del Garante (c.d. accesso "indiretto").

Accesso diretto

Come riportato più diffusamente nella *Relazione 2003*, il Codice ha stabilito (in linea con le scelte effettuate da gran parte dei paesi di "area Schengen") che l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del Sis, ossia il Dipartimento della pubblica sicurezza, fermo restando il diritto di proporre una segnalazione o un reclamo al Garante in caso di mancata o incompleta risposta.

In vista dell'entrata in vigore della nuova normativa il Garante, sulla base dell'esperienza, ha suggerito al Ministero dell'interno e all'Ufficio visti del Ministero degli affari esteri accorgimenti idonei ad assicurare ai richiedenti l'accesso un riscontro completo e tempestivo, anche attraverso il ricorso a moduli prestampati. A seguito delle indicazioni fornite dall'Autorità, il Dipartimento della pubblica sicurezza ha designato la Divisione N-SIS dell'Ufficio coordinamento e pianificazione delle forze di polizia quale ufficio preposto a ricevere le richieste di accesso, mentre il Ministero degli affari esteri ha comunicato alle ambasciate e alle cancellerie le necessarie misure operative, riformulando l'informativa da inserire sui provvedimenti di diniego di visto in modo da orientare più correttamente l'esercizio del diritto di verifica delle segnalazioni.

Il Garante ha reso nota al pubblico la nuova procedura (anche mediante *Newsletter*) pubblicando sul proprio sito *web*, in italiano e in inglese, una breve informativa con alcune indicazioni volte ad agevolare l'inoltro delle richieste di verifica, consultabile nella *home-page* del sito dell'Autorità (*www.garanteprivacy.it*); ad essa ha fatto riferimento anche il Ministero degli affari esteri nell'ambito delle direttive impartite agli uffici consolari.

Delle novità introdotte dal Codice l'Autorità ha poi informato le autorità nazionali di controllo sulla protezione dei dati, con le quali è stata instaurata una significativa collaborazione nell'ambito della procedura di coordinamento prevista dall'art. 114 della Convenzione di Schengen al fine di definire le indicazioni che tali autorità possono fornire agli interessati che richiedano assistenza per l'inoltro di richieste di accesso al SIS.

In proposito, l'Autorità ha registrato la fattiva collaborazione della Divisione N-SIS

del Dipartimento della pubblica sicurezza nell'applicazione della nuova normativa.

Su specifica indicazione fornita dall'Autorità, la Divisione N-SIS informa per conoscenza il Garante su ogni richiesta di accesso ricevuta e sul relativo riscontro fornito, in modo da consentire all'Autorità un efficace monitoraggio e controllo di tutte le richieste di accesso presentate. Quest'ultima, a sua volta, trasmette al predetto ufficio le richieste di semplice verifica dei dati che continuano a pervenire assai numerose probabilmente a causa di una ancora incompleta conoscenza (specie in paesi terzi) delle nuove modalità di accesso "diretto" introdotte dal Codice (dal 1° gennaio 2004 al 31 dicembre 2004 risultano pervenute al Garante circa 300 richieste).

Si tratta in gran parte di domande presentate a seguito di diniego del rilascio di visti, per lo più in conseguenza di segnalazioni dovute alla non ammissione nei Paesi Schengen di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera). In altri casi si tratta di asserite usurpazioni d'identità o di omonimie in relazione alle quali è stata ulteriormente rafforzata la collaborazione con il Centro visti del Ministero degli affari esteri e con la Direzione centrale per l'immigrazione e la polizia delle frontiere del Dipartimento della pubblica sicurezza.

Valutazione Schengen in Italia

Nei mesi di settembre e ottobre, l'Italia è stata oggetto della visita di valutazione da parte di gruppi di esperti del Consiglio dell'Unione europea. Il Consiglio ha infatti costituito da alcuni anni un gruppo per la valutazione Schengen che sta procedendo ad un esame, paese per paese, del funzionamento di tutti gli elementi che compongono il sistema: visti, frontiere esterne, SIS e SIRENE.

Una delle visite era espressamente dedicata alla verifica del rispetto delle norme italiane in materia di protezione dei dati personali; in particolare, ha riguardato le modalità di inserimento dei dati nel SIS nazionale, quelle di accesso ai dati contenuti nel sistema, le misure di protezione da accessi indesiderati e le misure di sicurezza dei sistemi e delle reti.

Attenzione è stata anche dedicata all'incontro con il Garante nella sua qualità di autorità nazionale di controllo sul SIS; dopo la presentazione svolta dal segretario generale dell'Autorità, sono state soddisfatte diverse domande tese a verificare il grado di effettiva indipendenza dell'Autorità (come, ad esempio, in merito a: disponibilità di una sede idonea, adeguatezza delle risorse finanziarie, possibilità di scelta del proprio personale e numero di persone in servizio) e le modalità di esercizio del suo ruolo di controllo sulla correttezza dei trattamenti.

Il rapporto redatto dagli esperti al termine della visita esprime una valutazione positiva pur contenendo alcuni inviti agli uffici di polizia che gestiscono il sistema informativo a migliorare la protezione dei dati da accessi non autorizzati e a controllare, in particolare, i dati inseriti dall'Italia nel SIS, numericamente superiori a quelli di qualsiasi altro paese Schengen, verificando la necessità del loro mantenimento nel sistema. Su questo aspetto il Garante stà eseguendo un dettagliato lavoro di verifica concordato con l'Autorità comune di controllo Schengen.

6.4. *Altri casi di intervento del Garante in relazione a diverse attività svolte dalle forze di polizia*

Foto segnaletiche

L'Autorità è nuovamente intervenuta in merito alla diffusione da parte di organi di polizia di immagini e, specialmente, di foto segnaletiche di persone coinvolte in attività di polizia (in particolare con riferimento ad una vicenda giudiziaria che ha coinvolto anche alcuni personaggi del mondo dello spettacolo). Il Garante ha sot-

tolineato –in linea con quanto già avvenuto in precedenti occasioni– che la diffusione di immagini di persone coinvolte in indagini o altri accertamenti è consentita agli organi di polizia solo per finalità di giustizia o di polizia e comunque nel rispetto della dignità della persona arrestata o altrimenti detenuta (cfr. art. 97, legge 22 aprile 1941, n. 633 sul diritto d'autore e art. 42-*bis*, legge 26 luglio 1975, n. 354). A seguito dell'intervento del Garante, le amministrazioni interessate hanno nuovamente richiamato il personale di polizia al rispetto della normativa vigente e delle cautele indicate dall'Autorità.

L'orientamento dell'Autorità ha trovato da ultimo conferma in una pronuncia della Corte europea dei diritti dell'uomo.

Trasmettere agli organi di stampa fotografie di una persona accusata in un procedimento penale costituisce infatti una violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo.

Il principio è stato affermato in una recente sentenza della Corte europea (50774/99, 11 gennaio 2005) originata dal ricorso di un'insegnante italiana –fermata e posta agli arresti domiciliari con l'accusa di associazione a delinquere, evasione fiscale e falso in bilancio– la cui fotografia, scattata durante le indagini, era stata diffusa nel corso di una conferenza stampa delle forze dell'ordine e quindi pubblicata su diverse edizioni di due quotidiani locali.

I giudici hanno messo in evidenza che, rispetto ad altri casi oggetto di precedenti pronunce della Corte (cfr. von Hannover/Germania, 59320/00, 24 giugno 2004), la fattispecie in esame presentava alcune peculiarità: essa, in primo luogo, non riguardava un personaggio pubblico; inoltre, la foto pubblicata proveniente dal fascicolo d'inchiesta era stata fornita ai giornali da agenti della Guardia di finanza.

Il fatto che nel caso di specie la ricorrente non fosse un personaggio pubblico giustifica –secondo la Corte– una contrazione della legittima "zona di interazione tra l'individuo e i terzi" (più ampia, evidentemente, nel caso di persone note) che non può espandersi in ragione del coinvolgimento della donna in un procedimento penale.

I giudici, inoltre, ravvisando l'inapplicabilità al caso di specie dell'art. 329 c.p.p. (obbligo del segreto per gli atti d'indagine), non hanno riscontrato la presenza di previsioni normative nell'ordinamento italiano che nella fattispecie in esame giustificassero, ai sensi del secondo comma dell'art. 8 della Convenzione, l'ingerenza nella vita privata della ricorrente.

Osservatorio appalti nel Mezzogiorno

Nell'ambito dei trattamenti svolti per finalità di polizia, il Ministero dell'interno ha sottoposto all'esame dell'Autorità la realizzazione di un sistema automatizzato di supporto alle decisioni per garantire trasparenza e sicurezza degli appalti nel Mezzogiorno che comporta l'acquisizione di dati da numerose altre pubbliche amministrazioni. Il Garante ha proposto l'avvio di un tavolo di lavoro finalizzato all'individuazione di una soluzione idonea a realizzare tale iniziativa nel pieno rispetto delle garanzie previste dal Codice (*Nota* 4 ottobre 2004).

L'Autorità ha altresì avviato specifici accertamenti in merito ad un progetto finanziato dall'Unione europea volto alla prevenzione ed alla repressione da parte delle forze di polizia del traffico di stupefacenti tra alcuni porti dell'Adriatico attraverso l'utilizzo di tecnologie informatiche di ultima generazione.

Cessione di fabbricati

Il Ministero dell'interno e la Questura di Genova hanno chiesto al Garante se i dati contenuti nelle comunicazioni di cessione di fabbricati di cui al decreto-legge 21 marzo 1978, n. 59, convertito in legge, con modificazioni, dalla legge 18 maggio 1978, n. 191, delle quali il sindaco è destinatario ai sensi dell'art. 15, comma 2, della l. n. 121/1981, potessero essere utilizzati dal comune per lo svol-

gimento di controlli di natura fiscale e tributaria.

L'Autorità ha chiarito che la disciplina da ultimo menzionata consente l'utilizzo delle informazioni contenute nel C.e.d. del Dipartimento di pubblica sicurezza esclusivamente per finalità di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità e ne vieta la circolazione all'interno della pubblica amministrazione (*Nota* 5 ottobre 2004).

Collaborazione con il Ministero dell'interno

L'Autorità è stata contattata dal Ministero dell'interno per approfondire le modalità di attuazione della normativa in materia protezione dei dati personali nell'ambito delle prefetture, con particolare riferimento ai trattamenti non finalizzati alla tutela della sicurezza e dell'ordine pubblico ovvero alla prevenzione, accertamento e repressione dei reati e, quindi, soggetti all'integrale applicazione del Codice.

Accesso ai dati anagrafici

Alcuni quesiti riguardano ancora le richieste delle autorità di pubblica sicurezza e delle forze di polizia volte ad acquisire informazioni e documenti riguardanti cittadini detenuti dagli uffici comunali. In proposito è stato in più occasioni ricordato che, fermo restando il divieto per le persone estranee all'ufficio di anagrafe di accedere all'ufficio stesso e, quindi, di procedere alla consultazione diretta degli atti anagrafici, le persone appositamente incaricate dall'autorità giudiziaria e gli appartenenti alle forze dell'ordine ed al Corpo della Guardia di finanza possono legittimamente consultare tali informazioni. In tal caso, tuttavia, i nominativi delle persone autorizzate ad effettuare la consultazione diretta degli atti anagrafici devono figurare in apposite richieste dell'ufficio o del comando di appartenenza, da esibire all'ufficiale di anagrafe unitamente ad un documento di riconoscimento (art. 37, d.P.R. 30 maggio 1989, n. 223).

Inoltre, il Codice prevede che, in conformità alla legge ed ai regolamenti, tale acquisizione possa altresì essere realizzata per via telematica attraverso convenzioni, anche con schemi tipo adottati dal Ministero dell'interno su conforme parere del Garante, a condizione che le modalità di collegamento previste assicurino un accesso selettivo ai soli dati necessari al perseguimento delle finalità di sicurezza ed ordine pubblico, nonché di prevenzione, accertamento e repressione dei reati (artt. 3, 11 e 54, del Codice).

Monitoraggio della spesa sanitaria

Prosegue, infine, l'attività di verifica dell'Autorità sui protocolli di intesa sottoscritti tra le regioni, le Asl e la Guardia di finanza ai fini del coordinamento dei controlli e dello scambio di informazioni in materia di spesa sanitaria che presentano diversi elementi critici sul piano della proporzionalità e liceità delle modalità di trattamento previste.

7 Attività giornalistica e mezzi di informazione

7.1. *Profili generali*

Il Codice in materia di protezione dei dati personali ha confermato il principio in base al quale chi esercita l'attività giornalistica o altra attività comunque riconducibile alla libera manifestazione del pensiero (inclusa l'espressione artistica e letteraria, come ora precisato dall'art. 136 del Codice) può trattare dati personali anche prescindendo dal consenso dell'interessato e, con riferimento ai dati sensibili e giudiziari, senza una preventiva autorizzazione di legge o del Garante. A fronte di queste esenzioni e deroghe si pone, tuttavia, l'obbligo di rispettare alcune condizioni: i limiti al diritto di cronaca già individuati in passato da una consolidata giurisprudenza; il requisito dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice); i principi previsti dal codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (adottato con provvedimento del Garante del 29 luglio 1998, all. A1 al Codice).

A distanza di sei anni dall'entrata in vigore del codice deontologico è stato costituito un gruppo di lavoro tra l'Autorità e l'Ordine nazionale dei giornalisti che si è occupato di analizzarne i principali profili applicativi. Per rispondere ai quesiti posti in quella sede, il 6 maggio 2004 il Garante ha approvato un documento *("Privacy e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti")* con il quale sono state fornite ulteriori precisazioni in merito al corretto utilizzo dei dati personali da parte dei giornalisti, specie in riferimento ad aspetti di particolare problematicità, quali la diffusione di fotografie, la pubblicazione dei nomi delle persone coinvolte in vicende giudiziarie, la diffusione di dati relativi allo stato di salute e alla vita sessuale, i margini di accessibilità da parte dei giornalisti alle informazioni detenute dalle pubbliche amministrazioni.

7.2. *Tutela dei minori*

La particolare tutela accordata ai minori dal Codice è stata richiamata dal Garante con interventi incisivi anche nel corso del 2004.

Si tratta di un settore in cui la vigente normativa in materia di tutela dei dati individua più chiaramente le coordinate entro cui il giornalista (o un soggetto ad esso equiparato ai sensi dell'art. 136 del Codice) è tenuto ad operare.

Il codice deontologico e la Carta di Treviso (da questo richiamata) stabiliscono con nettezza che il diritto del minore (anche quando si trovi coinvolto in fatti di cronaca che non costituiscono reato) alla riservatezza prevale sul diritto di critica e di cronaca. Il Codice ha rafforzato tali garanzie estendendo il divieto di pubblicare con qualsiasi mezzo notizie e immagini idonee a consentire l'identificazione di un minore (già affermato con l'art. 13, d.P.R. 22 settembre 1988, n. 448) anche nel caso in cui esso sia coinvolto a qualunque titolo in procedimenti giudiziari in materie diverse da quella penale (art. 50).

Il Garante ha adottato in proposito specifici provvedimenti di divieto della diffusione di dati idonei a rendere il minore, anche solo indirettamente, identificabile

(si pensi al caso, ad esempio, della pubblicazione di informazioni idonee ad identificare i genitori o afferenti al contesto ambientale e sociale in cui vive). Il divieto di diffusione del resto è posto, in caso di abusi sessuali subiti dal minore, anche da altre norme dell'ordinamento (*Provv.* 12 marzo 2004 e 6 aprile 2004).

Può inoltre rivelarsi necessaria l'adozione di cautele anche nella divulgazione dei dati identificativi di soggetti che risultano indagati per reati di siffatta natura pur quando non operino in tal senso specifiche limitazioni di legge (*Newsletter* 8-11 novembre 2004).

Come è stato chiarito nel documento del 6 maggio 2004, i limiti posti alla diffusione dei dati e delle immagini riguardanti i minori non sono assoluti; essa, infatti, può avvenire in casi particolari in cui un servizio giornalistico ritrae il minore in momenti di svago e di gioco o dà comunque positivo risalto a sue qualità e/o al contesto familiare in cui va formandosi, sempre che i dati siano stati raccolti nel rispetto del principio di correttezza. In linea con i principi generali della normativa in materia di tutela dei dati, il giornalista dovrà tuttavia valutare, anche in queste specifiche ipotesi, l'eventuale opposizione al trattamento manifestata dal minore o da chi ne esercita la potestà genitoriale.

7.3. *Cronache giudiziarie*

Come è noto, i dati giudiziari possono formare oggetto di trattamento per finalità di giornalismo (art. 137, comma 1, lett. *b*) del Codice), anche se nei limiti indicati dall'art. 12 del codice deontologico il quale, a sua volta, rinvia al principio di essenzialità dell'informazione. Tale disposizione va letta alla luce del Codice che estende ora la nozione di dati giudiziari, includendovi anche i dati idonei a rivelare la qualità di imputato e di indagato (art. 4, comma 1, lett. *e*), del Codice.

Continuano ad essere numerosi i reclami e le segnalazioni in relazione al trattamento di tali informazioni da parte degli organi di informazione. In questo ambito, indicazioni utili sono state fornite dal citato documento del 6 maggio 2004 che ha fornito chiarimenti sulle condizioni di liceità della diffusione di dati identificativi di persone arrestate o indagate, di foto segnaletiche e di altre immagini che documentano operazioni di arresto o altre attività processuali (ad es., la traduzione degli imputati), anche alla luce di norme diverse da quelle contenute nella normativa sulla protezione dei dati. Entro questi limiti è affidata alla responsabilità del giornalista la valutazione, caso per caso, dell'essenzialità della notizia (contenente il dato personale) in relazione all'interesse pubblico, ferma restando la completezza della medesima con riferimento alla corretta indicazione della fase del procedimento giudiziario di cui si dà notizia.

Non di rado i profili sollevati dai segnalanti in questo settore attengono alle modalità con cui vengono riportate le notizie, evidenziando possibili lesioni dell'onore e della reputazione dell'interessato piuttosto che problematiche attinenti alla protezione dei dati personali. Merita di essere segnalato a tal proposito il caso sottoposto all'attenzione del Garante (e in corso di accertamento) relativo alla diffusione del contenuto di intercettazioni telefoniche che consentivano l'accostamento del nome dell'interessato a quello dei componenti di un'organizzazione criminale. L'Autorità, ravvisata la liceità della raccolta dei dati dell'interessato in quanto desunti da atti conoscibili (ordinanza regolarmente depositata), ha ricordato nelle more che, fermo restando il diritto di chiedere la pubblicazione di una rettifica nei casi previsti dalla legge, la valutazione del carattere diffamatorio della notizia e dell'eventuale richiesta di risarcimento dei danni rimane di competenza dell'autorità giudiziaria ordinaria.

7.4. *Dati idonei a rivelare lo stato di salute*

Anche quest'anno l'Autorità ha richiamato i mezzi di informazione al rispetto della dignità e della libertà di autodeterminazione delle persone malate. In particolare, nel comunicato del 3 febbraio 2004 è stato stigmatizzato l'accanimento dei giornali sulla vicenda della donna che aveva espresso un rifiuto all'operazione di amputazione della gamba, ritenuta dai medici necessaria per salvarle la vita.

I medesimi principi sono alla base di un recente provvedimento con cui il Garante –al fine di prevenire il rischio di un possibile pregiudizio per l'interessato e in attesa di procedere ad ulteriori approfondimenti sul caso (art. 154, comma 1, lett. *d*), del Codice)– ha disposto il blocco temporaneo dell'ulteriore diffusione televisiva di immagini particolarmente invasive relative ad un uomo indigente, senza dimora, la cui identità sembrava corrispondere a quella di uno straniero assente da diversi anni dal proprio paese e di cui alcuni familiari avevano di recente intrapreso nuove ricerche (*Provv.* 8 novembre 2004).

7.5. *Libertà di informazione e personaggi pubblici*

Come più volte ricordato in passato, esistono alcuni margini più ampi per la diffusione di dati personali relativi a persone che godono di particolare notorietà (eventualmente anche in ambito locale), in ragione del ruolo o della funzione ricoperti. Questo diverso approccio opera solo quando l'informazione si riferisce al ruolo e alla vita pubblica di tali personaggi e non vengano diffuse informazioni relative a terzi. Tali principi, consolidatisi negli anni di applicazione del codice deontologico (artt. 10 e 11), sono stati ripresi nel documento del 6 maggio 2004, anche alla luce di quanto precisato dal Consiglio d'Europa (Dichiarazione del 12 febbraio 2004).

Questa "giurisprudenza" del Garante va ora misurata sulla recente sentenza della Corte europea dei diritti dell'uomo (von Hannover/Germania del 24 giugno 2004, citata nel par. 6.4) che si è pronunciata sulla controversa pubblicazione di una foto della principessa di Monaco ritratta in un momento della sua vita privata. La pronuncia conferma per un verso alcuni principi già espressi nella normativa italiana e ribaditi dal Garante in varie occasioni in merito ai presupposti di liceità per la raccolta (correttezza e trasparenza) e la diffusione delle fotografie nell'ambito di servizi giornalistici (tutela della dignità della persona; pertinenza e non eccedenza di eventuali dettagli fotografici). La decisione della Corte introduce però un'inedita distinzione tra trattamenti concernenti personaggi politici nell'esercizio delle loro funzioni e individui che, pur essendo figure pubbliche, non esercitano tali funzioni, invitando gli organi di informazione ad una maggiore cautela con riferimento alla diffusione di immagini e altri particolari che riguardano la vita privata di questi ultimi.

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

I diritti riconosciuti all'interessato dall'art. 7 del Codice trovano applicazione anche con riferimento ai trattamenti effettuati nell'ambito dell'attività giornalistica: al riguardo il Garante ha accolto due ricorsi presentati *ex* art. 145 del Codice in relazione a istanze di opposizione per motivi legittimi al trattamento rimaste insoddisfatte. La prima concerne la pubblicazione, da parte di un giornale locale, di dati idonei a rendere indirettamente identificabile una minore, vittima di reati sessuali

(*Provv.* 6 aprile 2004 sopra citato con cui, alla luce della speciale tutela accordata ai minori, è stato disposto il divieto di ulteriore trattamento dei dati). La seconda riguarda la ripetuta rievocazione, da parte di giornali a diffusione locale, di un episodio di grave aggressione subita in passato da una donna, ponendolo in connessione ad altri simili e più recenti fatti di cronaca. Il Garante, reputata fondata l'istanza dell'interessata, ha ritenuto ingiustificata la pubblicazione dei dati che la riguardavano (dati identificativi, residenza, particolari relativi allo stato di salute, fotografie) in ragione della loro eccedenza nonché dell'ampio lasso di tempo trascorso dall'episodio che aveva portato l'interessata all'attenzione della cronaca. L'Autorità ha così disposto il divieto di ulteriore trattamento dei dati della ricorrente e la cancellazione dei medesimi dalle pagine *web* delle relative testate giornalistiche (*Provv.* 15 aprile 2004).

Quest'ultima decisione ha riproposto la delicata tematica del cosiddetto "diritto all'oblio" su cui pure diversi quesiti, segnalazioni e reclami pervenuti al Garante hanno sollecitato un'ulteriore riflessione: in questo quadro giova ricordare le indicazioni contenute nel più volte citato documento del 6 maggio volte a sollecitare, da parte del giornalista, un'attenta ponderazione dell'essenzialità dell'informazione e del (rinnovato) interesse pubblico con riferimento a cronache di casi giudiziari risalenti nel tempo, con riguardo a persone condannate o assolte e, a maggior ragione, a soggetti estranei al processo rievocato (in questo senso possono segnalarsi alcuni accertamenti avviati dal Garante con riferimento a casi riproposti a distanza di tempo da una trasmissione televisiva).

Questo tema non può essere disgiunto dall'analisi dell'incidenza sul punto delle nuove tecnologie dell'informazione, in particolare nel caso di diffusione di informazioni tramite la rete Internet e conseguente utilizzo di motori di ricerca. Il nodo è venuto al pettine a proposito del ricorso proposto nei confronti dell'Autorità garante della concorrenza e del mercato cui si è già fatto cenno (v. par. 2.11).

8 Associazioni, movimenti politici e partiti

8.1. *Associazioni*

Con riferimento alle strutture associative, il trattamento dei dati personali non sensibili degli altri associati, o di soggetti che hanno contatti regolari con le associazioni, è consentito anche senza il consenso dell'interessato qualora riguardi il perseguimento di finalità lecite e sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione, o in presenza di uno degli ulteriori presupposti di liceità previsti dalla normativa sul trattamento dei dati personali (ad es., per obblighi di legge o per esigenze di difesa in sede giudiziaria).

Sindacati, patronati e Caaf

Nell'ambito delle diverse iniziative dell'Autorità sul tema del trattamento di dati personali da parte delle realtà associative è da ricordare, tra l'altro, l'incontro avuto con i rappresentanti delle principali organizzazioni sindacali, e degli enti di patronato e dei "Centri autorizzati assistenza fiscale" (Caaf) ad essi collegati, finalizzato alla revisione dei testi di informativa e consenso inseriti nelle tessere di adesione al sindacato. I soggetti intervenuti hanno chiesto il supporto dell'Ufficio del Garante allo scopo di sciogliere alcuni nodi interpretativi circa l'applicazione delle norme del Codice, con particolare riferimento alla possibilità di adottare un'informativa semplificata e di trattare in alcuni casi (in presenza di idonee garanzie) i dati senza il consenso degli interessati.

Con riferimento al trattamento dei dati all'interno delle strutture territoriali in cui si articolano le organizzazioni sindacali, il Garante ha richiamato la novità introdotta dal Codice riguardo alla facoltà di designare gli incaricati non solo nominativamente, ma anche mediante atti di preposizione a specifiche funzioni interne o unità organizzative che effettuano particolari trattamenti di dati, nell'ambito e a cura di titolari di strutture organizzative complesse che abbiano però chiarito per iscritto quali trattamenti di dati possono essere effettuati presso le singole articolazioni.

L'Autorità ha inoltre confermato l'obbligo, per i sindacati e per gli enti cd. collaterali (patronati e Caaf) di adottare le misure minime di sicurezza previste dal Codice e dal disciplinare tecnico, incluso il Documento programmatico per la sicurezza.

CONI

L'Ufficio ha anche reso un parere in ordine alla possibilità per il CONI di richiedere ad un ente di promozione sportiva riconosciuto a livello nazionale i dati relativi agli iscritti delle società affiliate all'ente. In proposito, nel richiamare le previsioni in materia di trattamento dei dati personali degli aderenti da parte delle associazioni, si è precisato che i soggetti pubblici, quale è il CONI, non devono richiedere il consenso degli interessati per il trattamento di dati personali effettuato nello svolgimento delle proprie funzioni istituzionali (*Nota* 24 maggio 2004).

Consorzi

È peculiare il caso esaminato dall'Autorità, su richiesta di un consorzio al fine di fornire alcuni chiarimenti in merito alle modalità di trattamento di taluni dati personali: si trattava di informazioni relative alla denominazione e alla sede del macello e delle aziende dove è avvenuto l'ingrasso, da riportare nell'etichettatura cd. facoltativa delle carni bovine, la quale contiene informazioni ulteriori rispetto a quelle

obbligatoriamente prescritte, allo scopo di migliorare la trasparenza delle condizioni di produzione e di commercializzazione delle carni bovine. In proposito, l'Autorità ha fatto presente che l'adesione al consorzio da parte delle singole imprese era avvenuta su base contrattuale e che, pertanto, la diffusione dei dati riprodotti nelle etichette (facoltativi rispetto alla normativa, ma obbligatori per gli aderenti al consorzio) non richiede il consenso degli interessati in quanto necessaria per eseguire obblighi derivanti dal contratto (qui consortile) (art. 24, comma 1, lett. *b*), del Codice) (*Nota* 1° luglio 2004).

8.2. *Movimenti politici e propaganda elettorale*

Il Garante –specie in prossimità di tornate di consultazioni elettorali– ha analizzato diverse questioni legate al trattamento dei dati personali effettuato da partiti e singoli candidati nell'ambito della propaganda politica.

In particolare, con un provvedimento di carattere generale (*Provv.* 12 febbraio 2004, pubblicato in *G.U.* 24 febbraio 2004, n. 45 e riprodotto anche in *Documentazione* par. 38) adottato in vista delle elezioni europee ed amministrative indette per il 12 e 13 giugno 2004, l'Autorità ha indicato i casi in cui partiti, movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui, al contrario, il consenso è necessario.

In tale occasione il Garante ha sottolineato che si può prescindere dal consenso nelle ipotesi in cui i dati utilizzati siano estratti da registri, elenchi, atti o documenti detenuti da un soggetto pubblico e accessibili liberamente in base ad un'espressa disposizione di legge o di regolamento.

Il candidato o l'organismo politico, sia quando acquisisca direttamente i dati sia allorché si avvalga dei servizi offerti da un privato, rivestendo comunque la qualifica di "titolare del trattamento", ha l'onere di verificare che gli interessati siano stati adeguatamente informati e abbiano prestato un consenso idoneo, validamente espresso solo se manifestato specificamente e se è stata resa all'interessato una previa informativa.

A tal proposito, merita di essere altresì ricordato il più recente provvedimento del 12 ottobre 2004, relativo all'invio di messaggi a contenuto propagandistico effettuato da una società per conto di una formazione politica. In tal caso l'Autorità ha sottolineato che, anche se l'invio di messaggi è avvenuto a nome di quest'ultima ad opera di un terzo, è la formazione politica medesima che è, e rimane, titolare del trattamento in questione; ciò in quanto essa assume le decisioni di fondo su finalità e modalità del trattamento preordinato all'invio del messaggio propagandistico.

Alla luce di tale principio, il Garante ha quindi prescritto alla formazione politica, a nome della quale la società aveva inviato *e-mail* per finalità promozionali senza aver acquisito il previo consenso dell'interessato, di fornire un idoneo riscontro alle richieste presentate ai sensi degli artt. 7 ed 8 del Codice.

Il Garante è stato anche interpellato in ordine alla liceità dell'invio di messaggi di posta elettronica a fini di propaganda elettorale da parte di società concessionarie di pubblicità ad utenti che avevano invece precedentemente conferito il loro esplicito consenso a ricevere solo comunicazioni di carattere commerciale e informativo. A tal proposito è stato rilevato che l'inserzione di messaggi di propaganda, in particolare nelle *Newsletter* tematiche richieste da soggetti cui è stata fornita una specifica informativa collegata al solo fine commerciale, non permette di considerare autorizzata anche la propaganda politica elettorale, poiché ciò contrasterebbe

con le particolari garanzie che il Codice prevede in tema di posta elettronica, differenti da quelle previste per la propaganda cartacea basata sull'utilizzo di registri ed elenchi pubblici accessibili a chiunque. È comunque praticabile (in luogo dell'inserzione di messaggi di propaganda all'interno di *Newsletter* tematiche) richiedere agli abbonati una manifestazione integrativa del consenso basata su un supplemento di informativa riferito alla propaganda politico-elettorale (*Nota* 25 marzo 2004).

Sempre a tale riguardo, e in linea con il predetto orientamento, in una successiva nota è stato precisato che non è sostenibile un accostamento tra le inserzioni pubblicitarie su quotidiani acquistati in modo anonimo presso un'edicola e i contenuti dei messaggi inviati nominativamente ad indirizzi di posta elettronica ad utenti che abbiano ricevuto un'informativa specifica riguardante solo attività commerciali o specifiche attività informative che nulla hanno a che vedere con la sfera politico-elettorale (*Nota* 7 aprile 2004).

9 Attività economiche

9.1. *Trattamenti in ambito bancario e finanziario*

Accesso ai dati personali in ambito bancario

Gli strumenti di tutela offerti dal Codice vengono utilizzati sempre più ampiamente nel settore bancario e finanziario: una problematica ricorrente è rappresentata dal rapporto tra il diritto di accesso ai dati personali detenuti da istituti di credito, specificamente disciplinato dagli artt. 7 e seguenti del Codice, ed il (diverso) diritto di ottenere copia della documentazione relativa ad operazioni bancarie, riconosciuto dall'art. 119, comma 4, d.lg. n. 385/1993 (T.U. in materia bancaria e creditizia).

In proposito, rispondendo anche ad alcune segnalazioni pervenute, nonché, in particolare, ad un quesito della Banca d'Italia, l'Autorità ha confermato l'alterità delle due figure in quanto il diritto di accesso previsto dal Codice si riferisce solo ai dati personali e non agli atti o documenti che li contengono, diversamente dal diritto, accordato dal menzionato art. 119, comma 4, d.lg. n. 385/1993, in base al quale il cliente, o colui che gli succede a qualunque titolo o colui che subentra nell'amministrazione dei suoi beni, possono *"ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni"* (*Nota* 6 agosto 2004).

Si è così ribadita la posizione consolidata dell'Autorità, precisando anche che il diritto di accesso ai dati personali comporta l'obbligo per il titolare del trattamento (in questi casi, le banche) di estrarre i dati e di trasporli, se vi è richiesta, su un supporto cartaceo o informatico, ma non l'obbligo di esibire o consegnare, anche in copia, gli atti e documenti che li contengono (a meno che risulti particolarmente difficoltosa l'estrazione dei dati dai medesimi atti o documenti e non sia parimenti possibile la loro trasmissione per via telematica: art. 10, comma 4, del Codice).

Il diritto di accesso riguarda, di norma, unicamente i dati riferiti all'interessato. Soltanto in casi particolari, nei quali risulti impossibile per la banca estrarre o trasporre singoli dati, può rendersi necessario far visionare o trasmettere, in tutto o in parte, atti o documenti che possono riguardare anche terzi: si tratta però di ipotesi eccezionali, ricorrenti solo quando i dati relativi al richiedente e ai terzi siano tra loro collegati in maniera tale che la scomposizione degli stessi o la privazione di alcuni elementi ne renderebbe incomprensibile la lettura (v. art. 10, comma 5, del Codice).

In base a tali disposizioni l'Autorità ha definito, ad esempio, il procedimento con il quale si è segnalata l'avvenuta consegna, da parte di un istituto di credito, della documentazione relativa ad estratti di un conto corrente, cointestato anche alla segnalante, agli eredi legittimi del genitore deceduto (contitolare di quel conto) che ne avevano fatto richiesta (*Nota* 24 marzo 2004).

Al di là dei più consueti rapporti di conto corrente, al diritto di accesso si fa ricorso anche in funzione prodromica a possibili azioni di responsabilità nei confronti degli istituti di credito: il Garante ha esaminato, ad esempio, il ricorso presentato da un cliente di una banca colpito da un'ingente perdita finanziaria dopo aver sottoscritto un investimento erroneamente reputato a basso rischio; il ricorrente intendeva accedere ai dati personali che lo riguardavano e, in particolare, a quelli contenuti nei documenti che ne evidenziavano obiettivi e propensione al rischio. Nel definire il procedimento, l'Autorità ha ribadito che il cliente può cono-

scere tutti i dati personali che lo riguardano detenuti da un istituto di credito e, in caso di operazioni finanziarie, può conoscere anche le informazioni eventualmente riportate nei documenti in cui sono indicati i rischi dell'investimento (*Provv.* 12 marzo 2004, v. *Newsletter* n. 209 del 5-25 aprile 2004). Come già riconosciuto in passato, le informazioni personali devono essere comunque comunicate in modo chiaro e intellegibile, fornendo altresì i criteri e i parametri per la comprensione dei codici eventualmente utilizzati.

Nella nozione di dato personale rientra *"ogni informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"* (art. 4, comma 1, lett. *b*), del Codice). Il Garante ha pertanto accolto un ricorso (*Provv.* 23 luglio 2004) avente ad oggetto l'accesso ai dati relativi alle registrazioni telefoniche degli ordini di negoziazione effettuati dal ricorrente, secondo le disposizioni di cui al regolamento Consob n. 11522/1998. Anche in tali fattispecie viene infatti effettuato un trattamento di dati personali (qui la voce del cliente) e sono pertanto proponibili le istanze *ex* art. 7 del Codice.

In ordine ai trattamenti effettuati da società emittenti carte di credito è stata poi esaminata una vicenda nella quale l'interessato aveva espressamente chiesto di conoscere anche i "criteri di selezione" adottati per valutare la richiesta della carta (*Provv.* del 10 giugno 2004); al riguardo l'Autorità ha sottolineato l'obbligo per il titolare del trattamento di comunicare all'interessato tutti i dati che lo riguardano, eventualmente detenuti anche in forma di punteggi negativi. Si sono ritenute inammissibili, invece, le richieste volte a conoscere alcune notizie attinenti a criteri organizzativi e gestionali del titolare del trattamento.

Accesso ai dati da parte di eredi dell'interessato

Un particolare profilo applicativo del diritto di accesso ai dati personali, che si presenta di frequente specialmente in ambito bancario e assicurativo, riguarda la possibilità che, nel caso di dati concernenti persone decedute, i diritti dell'interessato siano esercitati anche *"da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione"* (art. 9, comma 3, del Codice).

Si tratta di tematica delicata e complessa rispetto alla quale si è più volte richiamata la necessità di distinguere fra richieste, inammissibili dal punto di vista della protezione dei dati, volte ad ottenere specificamente e direttamente dati personali relativi a terzi (ad esempio, i nominativi dei beneficiari di contratti di assicurazione a favore di terzo o di destinatari di rimesse bancarie: v. già il *Provv.* 3 aprile 2002, in *Bollettino* n. 27 del 2002, p. 20 e ss.) ed istanze, fondate, dirette invece a conoscere dati e informazioni riferite al defunto: la banca è quindi tenuta a comunicare agli eredi in modo chiaro e comprensibile i dati relativi alla consistenza patrimoniale del defunto, a movimentazioni bancarie, saldi, depositi "al portatore", anche se estinti da terzi dopo la data del decesso, usando però l'accortezza di oscurare eventuali informazioni personali riferite a terzi (*Provv.* 20 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

Nelle diverse decisioni assunte in tema di accesso, il Garante ha ribadito la natura essenzialmente gratuita dell'esercizio dei diritti previsti dall'art. 7 del Codice. Peraltro, la complessità e l'estensione di alcune richieste di accesso in ambito bancario, sottolineata da diversi titolari, potrebbe portare in futuro l'Autorità, all'esito di un'adeguata istruttoria, ad adottare un provvedimento generale in tema di eventuali contributi spese forfettari a carico dell'interessato (contributo che, secondo quanto disposto dall'art. 10, comma 8, del Codice e in base ad una previa decisione generale del Garante, può essere chiesto dal titolare del trattamento, ad esempio qualora il riscontro alle richieste di accesso degli interessati comporti un notevole impiego

di mezzi in relazione all'entità o complessità delle istanze o comunque sia fatta richiesta della riproduzione dei dati cui si richiede l'accesso su speciali supporti).

Profili di liceità e correttezza

Attenzione particolare merita di essere attribuita ad un fenomeno relativo a modalità improprie di comunicazione talora adottate da banche, società finanziarie o società di recupero crediti, e consistenti nel contattare telefonicamente soggetti terzi –ad esempio abitanti nello stesso stabile– affinché riferiscano agli interessati di rivolgersi all'istituto per comunicazioni urgenti che li riguardano.

Si tratta di modalità di comunicazione che possono risultare lesive della riservatezza e della dignità degli interessati; l'Autorità ha pertanto richiamato l'attenzione di alcune banche sulla necessità di conformare le operazioni di trattamento ai principi di liceità e correttezza (art. 11, comma 1, lett. *a*), del Codice). In applicazione di tali principi, non dovranno essere effettuate comunicazioni alla clientela (relative anche a semplici richieste a terzi di riferire all'interessato di contattare la banca) per il tramite di condomini dello stesso stabile o vicini di casa, recando peraltro disturbo alla tranquillità di soggetti estranei al rapporto tra la banca e l'interessato; le banche e le società interessate, inoltre, sono state invitate a fornire apposite istruzioni in tal senso alle proprie strutture e dipendenti (*Note* 30 marzo 2004 e 25 ottobre 2004).

In un altro caso, l'Autorità ha rilevato un trattamento non corretto di dati personali da parte di una banca e di una società finanziaria, in occasione dell'addebito della rimessa interbancaria diretta (Rid) su un conto corrente diverso da quello indicato dal segnalante nell'ambito di una operazione di finanziamento (*Nota* 28 settembre 2004). La società finanziaria aveva infatti comunicato all'istituto di credito i dati indicati dal segnalante per la domiciliazione del Rid in modo inesatto ed incompleto, non fornendo né il numero di conto corrente prescelto per l'addebito, né il nominativo del terzo effettivamente intestatario di tale conto corrente (coobbligato per lo stesso rapporto di finanziamento). La banca, pur rilevando un'incompletezza dei dati comunicati, ha poi autonomamente proceduto, senza interpellare l'interessato, a domiciliare il Rid su un altro conto corrente non indicato a tal fine (cointestato al segnalante e ad un suo familiare), salvo poi sospendere l'addebito delle somme a seguito delle contestazioni del cliente.

Anche in questo caso, l'Autorità ha richiamato l'attenzione delle due società sulla necessità di impartire adeguate istruzioni al personale incaricato del trattamento per ridurre la probabilità che si verifichino errori analoghi e, comunque, per assicurare il pieno rispetto dei principi sanciti dal Codice in tema di correttezza del trattamento, di esattezza e di completezza dei dati.

9.2. *Trattamenti effettuati nell'ambito dei sistemi di informazione creditizia*

Conclusisi i lunghi e complessi lavori per la redazione del codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti, il testo preliminare del codice è stato dapprima sottoposto ad una consultazione pubblica e all'attenzione delle associazioni dei consumatori riunite nel Consiglio nazionale dei consumatori e utenti (Cncu) (recependone poi varie osservazioni) e, quindi, approvato dal Garante il 16 novembre 2004. Suscettibile di applicazione dal 1° gennaio 2005 (con d.m. 14 gennaio 2005 il Ministro della giustizia ha disposto l'allegazione al Codice), il codice è stato sottoscritto dalle associazioni rappresentative del settore creditizio e introduce un quadro articolato di garanzie per i soggetti che chiedono prestiti, mutui, dilazioni di pagamento, *leasing* e carte di credito.

Tra le novità, al di là della (significativa) nuova dizione –abbandonandosi la tradizionale denominazione *"centrali rischi private"* a vantaggio della locuzione *"sistemi di informazioni creditizie"* (Sic)–, merita segnalare le principali regole di comportamento che costituiscono condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali da parte delle società che li gestiscono e che li consultano (banche, società finanziarie e società di *leasing*), precisando che il codice deontologico non riguarda nella sua interezza i sistemi informativi gestiti da soggetti pubblici e, in particolare, il servizio di centralizzazione dei rischi gestito dalla Banca d'Italia (al quale continua ad applicarsi la specifica normativa di settore).

Per quanto riguarda, invece, il sistema centralizzato di rilevazione dei rischi di importo contenuto istituito con deliberazione Cicr del 3 maggio 1999 e attualmente gestito da Sia S.p.A. (Società interbancaria per l'automazione), relativo agli affidamenti di importo inferiore al limite minimo di censimento previsto per la Centrale della Banca d'Italia e superiore al limite massimo fissato per le operazioni di credito al consumo (cd."centralina"), con esclusione dei crediti in sofferenza, trovano applicazione, in quanto compatibili, alcuni principi stabiliti dal codice. Al riguardo, l'Autorità ha già avuto occasione di pronunciarsi precisando che quest'ultimo sistema (e il relativo trattamento di dati personali) non rientra nel campo di applicazione dell'art. 8, comma 2, lett. *d*), del Codice, per cui gli interessati possono esercitare i diritti di cui al precedente art. 7 (*Provv.* 27 luglio 2004).

Questi i principi basilari contenuti nel codice di deontologia:

- la fissazione delle finalità esclusive per le quali i sistemi di informazioni creditizie potranno essere utilizzati e consultati (tutela del credito e contenimento dei relativi rischi), con la contestuale preclusione del perseguimento di scopi ulteriori (ad esempio, relativi all'attività di *marketing* o ricerche di mercato);
- la precisazione delle categorie di dati che potranno essere trattate in questi sistemi; in particolare, si conferma la distinzione tra i sistemi, più diffusi, che registrano e forniscono informazioni su richieste e rapporti di finanziamento (ossia informazioni "di tipo positivo-negativo") e quelli che raccolgono solo dati "di tipo negativo", come i ritardi nei pagamenti (le cd. morosità) o situazioni più gravi di mancato rimborso del credito;
- la necessità di fornire idoneo preavviso al cliente prima di effettuare una segnalazione a contenuto negativo al sistema d'informazione creditizia;
- l'individuazione di precise regole per la segnalazione delle morosità;
- maggiore trasparenza nei confronti dei consumatori attraverso una completa informativa inserita in una modulistica più chiara: in allegato al codice deontologico vi è un modello unico per l'informativa –predisposto dal Garante ai sensi dell'art. 154, comma 1, lett. *c*), del Codice– basato su espressioni che aspirano ad essere chiare, semplici e di agevole comprensione, e che dovrà essere adottato da tutti gli operatori economici;
- la fissazione di tempi massimi di conservazione, distinti a seconda della natura della segnalazione effettuata. In particolare, per i dati di tipo "negativo": un anno per gli inadempimenti, poi regolarizzati, relativi a ritardi fino a due rate; due anni per ritardi superiori poi sanati; tre anni per inadempimenti non regolarizzati. Per i dati "positivi": ventiquattro mesi dalla cessazione del rapporto o dalla scadenza del contratto;
- la previsione che, in caso di ritardo nel fornire la risposta al consumatore che abbia esercitato il diritto d'accesso, la visualizzazione dei dati sia sospesa e che, in caso di controversie relative al rapporto sottostante la richiesta di finanziamento (riguardanti ad esempio inadempimenti del