I provvedimenti inibitori del 2008 [doc. *web* nn. 1544315, 1544326, 1544338, 1562780, 1562758] sono stati diretti non solo nei confronti di società che hanno effettuato tali attività direttamente, o tramite soggetti esterni nominati responsabili del trattamento, ma anche verso alcune tra le primarie società che hanno costituito e hanno venduto le banche dati contenenti le informazioni relative agli interessati da contattare telefonicamente per finalità promozionali.

Ai provvedimenti si è giunti dopo ripetuti richiami, istruttorie e ispezioni effettuate in alcuni casi anche con l'ausilio del Nucleo speciale *privacy*, avviate a seguito di reclami e segnalazioni ricevute dall'Autorità.

Dalla documentazione acquisita nel corso delle predette attività istruttorie, è emerso che le società che hanno fornito i *database* agli operatori telefonici avevano raccolto e ceduto a terzi i dati degli interessati senza informarli (o informandoli in maniera inadeguata) ed anche senza un loro preventivo specifico consenso. Una delle società offriva sul proprio sito i dati di oltre quindici milioni di famiglie italiane suddivise per reddito e stile di vita, senza che gli interessati fossero stati informati o avessero dato il loro assenso alla comunicazione dei dati a terzi.

Da parte loro le aziende e le compagnie telefoniche che hanno acquistato i dati e li hanno utilizzati a fini di *marketing* telefonico (il *cd.* "*teleselling*"), non si sono preoccupate di accertare, come prevede invece la disciplina sulla protezione dei dati, che gli abbonati avessero acconsentito alla comunicazione dei propri dati e al loro uso a fini commerciali.

Successivamente, con l'art. 44, comma 1-*bis* del decreto-legge 30 dicembre 2008, n. 207 (*cd. "decreto milleproroghe"*), convertito, con modificazioni, nella legge 27 febbraio 2009, n. 14 (*G.U.* 28 febbraio 2009 n. 49, S.O. 28), è stato stabilito che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.

Di seguito all'entrata in vigore di tale disposizione, che ha introdotto un regime derogatorio e transitorio in materia di *telemarketing*, il Garante ha ritenuto necessario interve-

nire al fine di chiarire rigorosamente i limiti entro i quali le società che operano nel settore possono avvalersi della deroga, precisando altresì le regole che le stesse dovranno seguire nell'uso dei dati degli abbonati.

Con il *provvedimento* del 12 marzo 2009 (*G.U.* 20 marzo 2009 n. 66 [doc. *web* n. 1598808]), l'Autorità ha così stabilito che le aziende e i *call center*, che intendano avvalersi della citata deroga e contattare gli utenti per fare promozioni e offerte commerciali utilizzando le predette banche dati, devono innanzitutto documentare in modo adeguato che la banca dati, costituita con i numeri telefonici e gli indirizzi degli abbonati, sia stata effettivamente creata prima del 1° agosto 2005, chiarendo altresì se il trattamento di dati venga effettuato anche per conto terzi. Le società e le aziende del settore, inoltre, sono tenute ad usare questi dati direttamente, senza possibilità di cederli a nessun titolo ad altre aziende.

Gli operatori che telefoneranno agli abbonati dovranno, poi, ad ogni contatto specificare per quale società chiamano e ricordare agli interessati i loro diritti, registrando immediatamente l'eventuale contrarietà dell'abbonato ad essere nuovamente contattato e comunicandogli l'identificativo dell'operatore.

I dati presenti nelle banche dati dovranno essere utilizzati solo a fini promozionali e non potranno in alcun modo essere usati per acquisire nuove informazioni o il consenso degli abbonati ad effettuare chiamate dopo la data del 31 dicembre 2009, poiché ciò determinerebbe di fatto la costituzione di nuove banche dati, andando al di là delle finalità stabilite dalla legge e prorogando, oltre il termine previsto, gli effetti della deroga temporanea.

Il Garante ha infine ricordato che il mancato rispetto del *provvedimento* comporta una sanzione amministrativa che va da 30.000 a 180.000 euro e che, nei casi più gravi, può raggiungere anche i 300.000 euro.

8.6.3. Telefonia

Rintracciabilità di persone disperse in montagna tramite localizzazione del cellulare

Anche nel 2008 diversi comuni hanno evidenziato che le ricerche di persone in pericolo, non in grado di comunicare la propria posizione, ad esempio perché in stato di incoscienza, potrebbero essere agevolate dalla possibilità di ottenere in tempo reale dal competente operatore telefonico la localizzazione del telefono cellulare delle persone stesse. I comuni

richiedenti hanno fatto riferimento all'attività svolta dal Corpo nazionale del soccorso alpino e speleologico (Cnsas), una delle strutture operative del Servizio nazionale della protezione civile (*cfr.* art. 11, comma 1, della l. n. 225/1992), che, infatti, ha spesso la concreta necessità di localizzare con urgenza persone disperse, in particolare in zone montane.

Pertanto, con il *provvedimento* del 19 dicembre 2008 [doc. *web* n. 1580543] il Garante ha chiarito che il Codice, nel caso vi sia la necessità di salvaguardare la vita o l'incolumità di una persona, consente alla società telefonica di comunicare senza indugio all'organismo di soccorso, anche senza il consenso dell'interessato, dati quali quelli concernenti i ponti e le celle attivate o *"agganciate"* dal telefono mobile della persona dispersa. La decisione ha, infatti, ad oggetto solo i dati relativi all'ubicazione diversi dai dati relativi al traffico, ossia i dati che possono essere reperiti sulla rete di comunicazione elettronica a prescindere da una comunicazione tra soggetti.

Pur riguardando il soccorso alpino, il *provvedimento* afferma princìpi suscettibili di essere applicati, con le dovute cautele, anche in altri casi in cui v'è esigenza di soccorso; l'Autorità ha chiarito, tuttavia, che i dati acquisiti dagli organismi di soccorso dovranno essere utilizzati solo per ricercare e soccorrere la persona dispersa.

L'Autorità ha inoltre ricordato che i servizi abilitati a ricevere le chiamate di emergenza possono comunque trattare i dati relativi all'ubicazione dei telefoni relativi a chi chiama, anche quando l'utente o l'abbonato abbia già rifiutato o omesso di prestare il consenso (*cfr.* considerando 36 e art. 10, comma 1, lett. *b*) della Direttiva 2002/58/Ce e art. 127, comma 4, del Codice).

9. Associazioni e partiti politici

Nel corso dell'anno l'Autorità ha avuto modo di approfondire la tematica del trattamento dei dati personali all'interno delle realtà associative, nelle quali si esplicano i diritti fondamentali della persona e più intensa può essere la circolazione di informazioni personali, talora assai delicate (in quanto riferite a scelte, opinioni o condizioni individuali spesso riconducibili al novero dei dati sensibili).

Affissione nella bacheca associativa di provvedimenti disciplinari

Una reclamante ha lamentato che dati personali contenuti in provvedimenti disciplinari emanati nei suoi confronti da una federazione sportiva erano stati affissi in spazi liberamente accessibili ai soci di un circolo sportivo (affiliata alla medesima federazione). La pubblicazione dei provvedimenti disciplinari non sarebbe risultata consentita dallo statuto del circolo, né doverosa in attuazione di specifiche norme federali.

Dagli elementi acquisiti si è ritenuto che l'affissione non trovasse giustificazione nelle norme statutarie vigenti e che l'interessata non avesse ricevuto idonea informativa in ordine a tale eventualità.

In termini generali, il Codice rimette alle determinazioni adottate da organismi senza scopo di lucro le modalità ed i limiti nella divulgazione di dati personali relativi agli iscritti; ciò per consentire agli stessi iscritti di valutare in concreto – al di là delle necessarie misure organizzative da predisporre a livello associativo – le possibili *"ricadute"* individuali legate ad una più ampia circolazione delle informazioni anche nei confronti di tutti gli altri associati (talvolta di numero assai elevato) oltre che la natura (più o meno sensibile) delle informazioni suscettibili di comunicazione.

Peraltro, tenuto conto che i provvedimenti disciplinari emanati erano stati rimossi dalla bacheca e che il trattamento dei dati ivi contenuti era comunque cessato prima ancora che l'associazione avesse notizia del reclamo, non si sono ravvisati i presupposti per l'adozione di provvedimenti da parte dell'Autorità (art. 11, comma 1, lett. *d*), Reg. Garante n. 1/2007), fermi restando gli eventuali danni derivati all'interessata dall'avvenuta divulgazione di dati personali a sé riferiti (*Note* 19 agosto 2008 - 9 ottobre 2008).

Comunicazione ad un socio di dati personali riferiti agli associati

L'iscritto ad una federazione ha posto un quesito in tema di accesso ai dati personali degli altri associati (in forma di elenco, comprensivo di nominativi ed indirizzi) per l'esercizio di prerogative legate all'appartenenza all'associazione.

Al riguardo l'associazione, in base all'art. 26, comma 4, lett. *a*), del Codice, può determinare *"il se e il come"* della conoscibilità, all'interno della realtà associativa, dei dati personali degli aderenti, anche in difetto del consenso dei singoli associati, a condizione che la comunicazione avvenga nel rispetto di *"idonee garanzie"* determinate dalla stessa associazione in relazione ai trattamenti effettuati e che l'associazione medesima abbia reso note agli interessati, all'atto dell'informativa rilasciata ai sensi dell'art. 13 del Codice, le determinazioni in merito adottate, prevedendo espressamente le modalità di utilizzo dei dati (che dovranno essere comunque pertinenti e non eccedenti rispetto alle finalità sottese alla richiesta: art. 11, comma 1, lett. *d*), del Codice).

Resta comunque salva la possibilità per ciascuna associazione di individuare modalità diverse per veicolare messaggi o comunicazioni di singoli associati all'interno della compagine associativa (facendo così da tramite dei singoli iscritti), nelle forme ritenute più opportune senza che ciò comporti la comunicazione di indirizzari di tutti gli iscritti a taluni di essi (*Nota* del 24 giugno 2008).

Movimenti politici

Alcuni segnalanti hanno lamentato di aver ricevuto una tessera di iscrizione ad un Movimento politico senza averla mai richiesta (né aver pagato la relativa quota) ed in assenza della prescritta informativa.

In riscontro a quanto al riguardo richiesto dall'Autorità, il Movimento ha dichiarato di aver cancellato immediatamente i dati personali dei segnalanti a seguito di alcune comunicazioni ricevute da parte degli stessi. In ogni caso, uno dei segnalanti sarebbe stato in continuo contatto con l'organizzazione, in qualità diverse, con costante frequentazione dei relativi uffici; in occasione del Congresso nazionale del Movimento, uno dei segnalanti avrebbe richiesto il rinnovo della tessera anche per l'altro; le tessere *"scadute"* non sarebbero state ricusate dagli interessati. Inoltre il consenso dei segnalanti alla consegna della tessera dell'organizzazione sarebbe stato acquisito (verbalmente) da due addette alla segreteria, senza compilazione del relativo modulo di adesione (data anche la conoscenza personale degli interessati).

A conclusione dell'attività istruttoria espletata, non risultando comprovata l'avvenuta ricezione, da parte dell'organizzazione, di una domanda corredata dai dati anagrafici degli interessati (come richiesto dallo statuto), né che tale formalità potesse rientrare tra le garanzie previste ai fini dell'esonero dall'acquisizione del consenso scritto degli interessati (art. 26, comma 4, lett. *a*), del Codice), l'Autorità ha prescritto al Movimento di accertare l'effettiva cancellazione dei dati dei segnalanti da parte delle strutture locali, nonché di prevedere idonee garanzie in caso di trattamenti effettuati prescindendo dal consenso scritto degli interessati. Non è risultata invece comprovata, diversamente da quanto lamentato dai segnalanti, la violazione della disciplina di protezione dei dati avente ad oggetto l'abusiva utilizzazione di informazioni per finalità di rilascio di una tessera di iscrizione al Movimento, tenuto conto delle dichiarazioni univocamente rese in proposito dalle addette alla segreteria dell'organizzazione (*Provv.* 15 febbraio 2008 [doc. *web* n. 1523069]).

Propaganda politica ed elettorale

Anche nel 2008, come in analoghe occasioni, il Garante – in vista delle consultazioni elettorali europee, amministrative e referendarie di giugno 2009 – ha adottato un *provvedimento* generale (*Provv.* 2 aprile 2009, in *G.U.* 11 aprile 2009, n. 85 [doc. *web* n. 1603863]) recante misure in materia di propaganda elettorale.

In tale documento sono state richiamate integralmente le prescrizioni contenute nel *provvedimento* generale del 7 settembre 2005 (*G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613]) sul trattamento dei dati senza rendere l'informativa agli interessati.

In particolare, è stato previsto che, decorsa la data del 30 settembre 2009, partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati possono continuare a trattare temporaneamente (anche mediante mera conservazione) i dati personali lecitamente raccolti secondo le modalità indicate nel predetto *provvedimento* del 7 settembre 2005, informando gli interessati entro il 31 dicembre 2009, nei modi previsti dal Codice.

Dai predetti provvedimenti emergono ulteriori princìpi che devono essere osservati da partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati che intraprendono iniziative di selezione di candidati alle elezioni, di comunicazione e di propaganda elettorale.

In particolare, senza il preventivo consenso degli interessati, possono essere utilizzati solo i dati contenuti nelle fonti documentali detenute da soggetti pubblici, liberamente accessibili a chiunque in base a una specifica norma (*ad es.*, le liste elettorali e gli altri elenchi e registri in materia di elettorato attivo e passivo).

I titolari di cariche elettive possono utilizzare le informazioni raccolte nel quadro delle relazioni interpersonali con cittadini ed elettori senza il preventivo consenso degli interessati; tuttavia, non sono legittimati ad ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi *"dedicati"* da utilizzare per attività di propaganda elettorale, così come non sono utilizzabili i dati raccolti nell'esercizio di attività professionali e di impresa.

Nell'ambito di partiti, organismi politici, comitati di promotori e sostenitori, si possono utilizzare, senza apposito consenso, dati personali relativi a iscritti e aderenti, nonché ad altri soggetti con cui si intrattengono regolari contatti. Altri enti, associazioni ed organismi senza scopo di lucro (associazioni sindacali, professionali, sportive, di categoria, *ecc.*), possono prevedere tra i propri scopi anche le finalità di propaganda elettorale che, se perseguite direttamente dai medesimi enti, organismi o associazioni, non richiedono il consenso.

I dati estratti dagli elenchi telefonici possono essere invece trattati a fini di propaganda elettorale per l'invio di posta ordinaria o di chiamate telefoniche effettuate da un operatore, a seconda dei simboli apposti sull'elenco. Qualora si ricorra all'invio di *fax*, di messaggi *Sms* e *Mms*, o di *e-mail*, nonché a chiamate telefoniche senza l'intervento di un operatore oppure a chiamate a terminali di telefonia mobile, non è possibile svolgere attività di propaganda politica senza il consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente gli scopi per i quali i dati sono utilizzati.

L'eventuale acquisizione dei dati personali da un terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, compresi quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dal verificare, anche a campione e avvalendosi del mandatario elettorale, che il terzo: a) abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda e abbia

ottenuto il loro consenso idoneo ed esplicito; b) non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili. Queste cautele vanno adottate anche quando il terzo, oltre a fornire i dati, svolge le funzioni di responsabile del trattamento designato da chi effettua la propaganda.

10. Le attività economiche e i rapporti di lavoro

10.1. Settore bancario

Anche nel 2008 sono pervenuti numerosi reclami e segnalazioni relativi all'attività bancaria, molti su aspetti già trattati nelle *"Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario"* (*Provv.* 25 ottobre 2007, *G.U.* 23 novembre 2007 n. 273 [doc. *web* n. 1457247]).

Banche, videosorveglianza e registrazione delle impronte digitali

Si è riferito nella *Relazione* 2007 (*p.* 88) degli accertamenti eseguiti nel 2008 per verificare il rispetto delle prescrizioni impartite nel *provvedimento* del 27 ottobre 2005 [doc. *web* n. 1246675] sul trattamento di dati personali dei clienti (immagini del volto e delle impronte digitali) per accedere all'interno delle filiali.

Attività bancaria ed elenchi di sospetti terroristi

Il cliente di un istituto di credito ha segnalato che, recatosi presso la propria banca per negoziare un assegno, dopo essere stato identificato, gli veniva comunicato dall'operatore di sportello, e confermato anche dal direttore, che l'operazione non poteva essere eseguita, poiché il suo nome e cognome risultavano inseriti *"nell'elenco dei latitanti terroristi"*. All'esito dell'attività istruttoria, il Garante ha precisato che nel caso di specie la banca non aveva utilizzato tutte le informazioni pertinenti, complete e non eccedenti in concreto disponibili nel conseguimento della legittima finalità perseguita (come prescritto dall'art. 11, comma 1, lett. *d*), del Codice). Tali informazioni, contenute nella lista formata e aggiornata periodicamente anche a cura dell'Ufficio italiano dei cambi, non si limitano infatti al solo nome e cognome del sospetto terrorista, ma includono dati ulteriori, quali data, luogo di nascita e codice fiscale. Secondo le indicazioni dell'Uic (provvedimento Uic, 9 novembre 2001, in *http://uif.bancaditalia.it/UICFEWebroot/*) tra i dati identificativi sono comprese le cariche, le qualifiche e ogni altro dato riferito nelle liste ai soggetti venuti in rilievo. A quest'ultimo riguardo, la coincidenza non sussiste qualora l'intermediario, sulla base di informazioni certe e secondo valutazioni di ragionevolezza, possa escludere che tali cariche e qualifiche siano attribuibili al cliente in quanto incompatibili con il tenore di vita ed ogni sua altra caratteristica oggettiva e soggettiva (*cfr. cit.* provvedimento Uic punto 2.4).

Il Garante ha pertanto prescritto alla banca di adottare tutte le misure necessarie ad assicurare il rispetto dei princìpi di qualità dei dati e correttezza del trattamento (art. 11 del Codice), adattando i sistemi operativi in modo da trattare nella stessa unità di tempo tutte le informazioni pertinenti e non eccedenti, in concreto disponibili, nel conseguimento della legittima finalità perseguita (*Provv.* 7 febbraio 2008 [doc. *web* n. 1523046]).

Home banking

In una segnalazione, un correntista ha lamentato che la *password* per l'accesso *on-line* ai conti correnti, di cinque caratteri numerici, sarebbe in contrasto con la regola 5 del *"Disciplinare tecnico in materia di misure minime di sicurezza"* Allegato B. al Codice, che prevede come misura minima di sicurezza l'utilizzo di una *password* di otto caratteri.

Dagli accertamenti, effettuati anche *in loco*, è emerso che la clientela del servizio di *home banking* riceve una tessera (*Password card*) contenente quaranta codici numerici composti da sei cifre decimali, ciascuno dei quali può essere utilizzato una sola volta in occasione di ciascuna operazione dispositiva; una volta esauriti i codici a disposizione, viene inviata al cliente una nuova scheda. Le modalità adottate dall'istituto di credito non sono state comunque ritenute in contrasto con la disciplina di protezione dei dati personali anche in considerazione della circostanza che l'Allegato B. al Codice riguarda le modalità tecniche che devono essere adottate dal titolare del trattamento e, quindi, la menzionata regola 5 si riferisce alle credenziali di autenticazione assegnate agli incaricati del trattamento e non ad altri soggetti, quali la clientela della banca che accede *on-line* ai servizi bancari (*Nota* 27 febbraio 2008).

Fusioni bancarie

Nel 2008 due istituti di credito hanno chiesto di essere esonerati dall'obbligo di rendere l'informativa agli interessati (clienti, fornitori e dipendenti) in relazione ai trattamenti di dati personali conseguenti alle operazioni di ristrutturazione societaria.

Al riguardo, il Garante non ha ritenuto necessaria l'adozione di provvedimenti ai sensi dell'art. 13, comma 5 del Codice, ma con due *provvedimenti* (11 dicembre 2008 [doc. *web* n. 1584328] e 19 dicembre 2008 [doc. *web* n. 1584272]), ha prescritto alle banche interessate dalle operazioni societarie di fornire agli interessati – sia attraverso il sito *web* delle banche, sia con comunicazione individualizzata in occasione della prima circostanza utile di contatto – la nuova denominazione del titolare del trattamento e gli estremi identifica-

tivi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali.

Tale soluzione (peraltro coerente con l'orientamento della Cass. Sez. un., 8 febbraio 2006, n. 2637) deriva dalla considerazione che per effetto della fusione per incorporazione, la banca incorporante assume i diritti e gli obblighi della banca incorporata, e diviene (unico) titolare del trattamento senza che si configuri alcuna (nuova) raccolta di dati. La continuità nei rapporti in corrispondenza di tali operazioni societarie posti in essere dalle banche, risulta conforme anche alla disciplina di settore contenuta nell'art. 57, comma 4, del d.lg. 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia).

Trattamenti di dati personali e valutazione di adeguatezza e appropriatezza delle operazioni o dei servizi di investimento

Nel 2008 alcune associazioni di consumatori e privati cittadini si sono rivolti all'Autorità in merito alla raccolta di dati personali dei clienti effettuata, attraverso questionari prestampati, da parte di operatori bancari e finanziari che, per dare esecuzione a servizi di consulenza, raccolgono presso la clientela informazioni volte a valutare l'adeguatezza e l'appropriatezza delle operazioni o dei servizi di investimento raccomandati agli stessi clienti. In tal modo, gli operatori danno attuazione alla normativa di settore, che ha recepito le direttive comunitarie (2004/39/Ce del 21 aprile 2004, relativa ai princìpi quadro e 2006/73/Ce del 10 agosto 2006, recante le modalità di esecuzione della precedente) attraverso il Regolamento Consob di cui alla delibera n. 16190 del 29 ottobre 2007 in conformità alla previsione contenuta nell'art. 6, comma 2, lett. *b*), punto 1, d.lg. n. 59/1998 (come modificato dall'art. 2, d.lg. 17 settembre 2007, n. 164).

Al riguardo, l'Autorità ha precisato che le imprese di investimento devono rispettare la disciplina di protezione dei dati personali, in particolare, i princìpi di pertinenza e non eccedenza rispetto alla finalità legittimamente perseguita, in linea anche con le direttive comunitarie e la stessa disciplina nazionale di recepimento (art. 35, parr. 3 e 4, Direttiva 2006/73/Ce; art. 39, commi 2, 3 e 4, Reg. Consob) ed i dati raccolti non possono essere utilizzati dalle imprese di investimento per finalità incompatibili rispetto a quelle che ne hanno determinato la raccolta (art. 11, comma 1, lett. *d*), del Codice). È pertanto necessaria un'approfondita previa valutazione in ordine alla pertinenza e non eccedenza dei dati

personali trattati nell'ambito del servizio di consulenza e di gestione del portafoglio, anzitutto da parte dell'impresa di investimento, tenuto conto delle circostanze concrete relative a ciascuna delle operazioni effettuate o dei servizi resi. Per la mera esecuzione di ordini impartiti dal cliente (*cd. "execution only"*) la normativa vigente non prevede, ricorrendo le indicate condizioni, la raccolta delle menzionate informazioni (art. 43 Reg. Consob; art. 19, *par.* 6, Direttiva 2004/39/Ce) (*Nota* 26 marzo 2009).

Comunicazione a terzi di dati riferiti alla clientela

Alcuni casi (taluni dei quali in corso di approfondimento) hanno riguardato l'asserita comunicazione a terzi da parte della banca di dati personali dei clienti, anche con riferimento al successivo utilizzo di tali informazioni nell'ambito di procedimenti giudiziari.

In particolare in un reclamo è stata lamentata la comunicazione da parte di una banca, attraverso la produzione documentale e gli atti depositati in un procedimento giudiziario promosso dal cliente contro la stessa banca, di dati personali relativi non solo all'attore (che comunque lamentava l'eccedenza e non pertinenza di dati allo stesso riferiti), ma anche a soggetti estranei al procedimento giudiziario, quali il figlio (cointestatario con il padre del conto corrente oggetto del giudizio) e la nuora.

In via preliminare, l'Autorità ha rilevato che il giudizio sulla rilevanza e ammissibilità delle prove in giudizio (ivi compresi i profili derivanti dall'applicazione della disciplina sulla protezione dei dati personali) spetta all'autorità giudiziaria (art. 160, comma 6 del Codice, in conformità, dal punto di vista sistematico, con l'art. 116, primo comma c.p.c.). Nel caso in esame, il trattamento dei dati effettuato dalla banca convenuta nei riguardi del proprio cliente risultava essere avvenuto per fare *"valere o difendere un diritto in sede giudiziaria"* e, pertanto, non richiedeva il consenso degli interessati (art. 24, comma 1, lett. *f*), del Codice). Infatti, le informazioni trattate erano funzionali a valutare l'esperienza in materia di investimenti in strumenti finanziari, la situazione finanziaria, gli obiettivi di investimento, nonché la propensione al rischio del cliente. Analoghe considerazioni sono stata fatte in relazione ai confronti dei dati del figlio dell'attore, che era, comunque, cointestatario del conto oggetto del procedimento. Una diversa valutazione ha riguardato, invece, il trattamento di dati personali relativi alla nuora dell'attore, che risulta in contrasto con il principio di pertinenza e non eccedenza (oltre che con quello di finalità) dal

momento che la stessa non è risultata ad alcun titolo parte del contratto di investimento, né destinataria degli effetti economici dell'operazione (*Nota* 23 ottobre 2008).

Produzione ed esibizione di documentazione contenente informazioni bancarie in giudizio

In una segnalazione il socio di maggioranza di una società in nome collettivo – divenuto erede anche della quota di minoranza – ha contestato le modalità con le quali una banca, in esecuzione di una pronuncia dell'autorità giudiziaria, aveva fornito al notaio procedente alla formazione dell'inventario di beni ereditari dati in suo possesso riferibili al *de cuius* e relativi a prelievi e versamenti a qualunque titolo effettuati entro determinati limiti temporali. In particolare, la segnalante ha lamentato la comunicazione da parte della banca di dati inerenti operazioni riferite ad un conto corrente non intestato personalmente al defunto.

Dagli atti, tuttavia, è emerso che, ancorché nel momento in cui la banca ha dato esecuzione all'ordine impartitole dal giudice, il conto fosse già intestato all'impresa individuale di cui era titolare la segnalante (subentrata nel relativo contratto di conto corrente per effetto dell'intervenuto scioglimento della società), i dati personali comunicati si riferivano solo alle operazioni effettuate sul conto corrente bancario finché era stato intestato alla società di cui era socio il *de cuius*, senza riguardare l'impresa individuale. Considerato, inoltre, che la banca era tenuta a fornire i dati relativi a movimenti bancari *"a qualunque titolo"* riferibili al defunto e tenuto altresì conto della peculiare ragione sociale adottata dalla società, della quale il *de cuius* era socio, l'Autorità ha escluso che nel caso di specie la comunicazione da parte della banca sia avvenuta in violazione del Codice (*cfr.* le *"Linee-guida in materia di trattamento dei dati personali della clientela in ambito bancario"* per il caso in cui la comunicazione avvenga, nelle forme previste dalla legge, nei confronti dell'autorità giudiziaria - punto 3.3. del *provvedimento*) (*Nota* 12 novembre 2008).

In un altro caso, la segnalante ha chiesto l'intervento del Garante in relazione all'inottemperanza da parte di due istituti di credito ad un ordine di esibizione emesso dal giudice ai sensi dell'art. 201 c.p.c.. L'Autorità, nel richiamarsi al punto 3.3. delle menzionate *"Linee-guida"* ha invitato la segnalante ad attivare, ogni rimedio riconosciuto dall'ordinamento giuridico nei confronti dell'inottemperanza del terzo al provvedimento esibitorio, non essendo riconosciuta al riguardo alcuna competenza al Garante (*Nota* 6 novembre 2008).

Un'ulteriore segnalazione ha riguardato la produzione da parte di una banca, nel corso di un procedimento giudiziario contro la banca medesima, delle movimentazioni del conto corrente intestato alla segnalante, contenente informazioni relative ad operazioni bancarie non inerenti il giudizio.

Al riguardo, l'Autorità ha richiamato i princìpi contenuti nelle *"Linee-guida"* in materia, con specifico riferimento al fatto che in giudizio possono essere prodotti solo i dati pertinenti all'esigenza di far valere o difendere un diritto dell'istituto di credito, evitando proprio l'ingiustificata produzione di interi tabulati (*ad es.*, interi estratti conto) contenenti dati personali (a volte anche riferiti a terzi) non rilevanti per le citate finalità di difesa (punto 4, anche in relazione al contenuto dell'art. 160, comma 6, del Codice). Nel caso di specie si è quindi ritenuto che la banca avrebbe dovuto oscurare, in tutto o in parte, le informazioni bancarie non pertinenti rispetto alla controversia pendente, restando in ogni caso impregiudicato il potere del giudice di richiedere (specie in caso di contestazione) la produzione integrale della documentazione (*Nota* del 17 ottobre 2008).

Abbandono di documentazione bancaria e misure di sicurezza

In un reclamo è stata lamentata la diffusione di dati personali di due clienti di una banca conseguente all'abbandono, in occasione del rilascio dei locali ove operava uno sportello dell'istituto di credito, di alcuni documenti prodotti in occasione dell'istruzione di una richiesta di mutuo alla quale i reclamanti avevano successivamente rinunciato. Da una complessa attività istruttoria (anche con accertamenti ispettivi) è emerso che i menzionati documenti, contenenti dati personali non sensibili né giudiziari, erano stati rinvenuti dal responsabile della sicurezza dello *"store"* dove era ubicato lo sportello bancario in un armadio che la banca si era impegnata a cedere con altre suppellettili ad un istituto di credito subentrato nell'utilizzo dello sportello. Gli accertamenti espletati hanno consentito di appurare che la banca aveva adottato, all'epoca dell'episodio segnalato, misure di sicurezza organizzative *"minime"* a protezione dei dati dei clienti trattati senza l'ausilio di strumenti elettronici già conformi a quanto attualmente prescritto dall'art. 35 del Codice e dalla regola 27 dell'Allegato B. al Codice, impartendo istruzioni scritte ai lavoratori incaricati del trattamento. Poiché tali istruzioni non avevano formato oggetto di rivisitazione dopo il 2000, si è rappresentato alla banca la necessità di aggiornarle alla luce della

maggiore articolazione della disciplina in materia contenuta nel Codice e del punto 2.1. delle *"Linee-guida"*. La banca è stata poi invitata ad adottare, ai sensi dell'art. 31 del Codice, misure di sicurezza idonee per il trattamento di dati personali diversi da quelli sensibili e/o giudiziari effettuato senza l'ausilio di strumenti elettronici, con specifico riferimento alla predisposizione di specifiche procedure atte a garantire un'adeguata vigilanza da parte del titolare del trattamento sull'operato del personale incaricato del trattamento dei dati personali dei clienti, con particolare riguardo all'ipotesi di cessazione dell'attività bancaria presso sportelli periferici detenuti in locazione (*Note* del 18 dicembre 2008 e 2 marzo 2009).

Un'altra segnalazione ha riguardato la diffusione di dati personali riferiti a taluni correntisti, contenuti in documenti rinvenuti accidentalmente da un passante sulla via ove ha sede la banca. Dagli elementi acquisiti *in loco* è emerso che la banca aveva adottato misure di sicurezza conformi al Codice e che per un disguido la documentazione era stata inserita nei contenitori per la raccolta della spazzatura ordinaria anziché in quelli destinati al macero. La banca è stata invitata ad assicurare (tramite l'attenta vigilanza sull'operato degli incaricati e in occasione delle iniziative formative prescritte dalla regola 19.6 dell'Allegato B. al Codice) la scrupolosa attuazione delle istruzioni impartite (con specifico riguardo a quelle riguardanti la custodia, la conservazione, nonché la restituzione dei documenti contenenti dati personali al termine del relativo trattamento) da parte degli incaricati del trattamento (*Nota* 2 marzo 2009).

Coordinate bancarie in fatturazione e principio di pertinenza e non eccedenza

In una segnalazione si è contestata l'avvenuta inclusione, tra i dati contenuti nella fattura recapitata da una società per la fruizione del servizio di telefonia, del numero di conto corrente riferito alla segnalante, ritenuto eccedente rispetto alla finalità perseguita (ai fini della fatturazione del servizio, infatti, sarebbe stato sufficiente, a detta della medesima segnalante, la mera indicazione dell'istituto creditizio presso il quale effettuare il prelievo). Al riguardo, è stato precisato che l'indicazione di detto numero in sede di fatturazione del servizio appare eccedente, poiché il corretto addebito della somma fatturata può essere riscontrato già dall'estratto conto inviato al cliente dalla banca domiciliataria. A conferma di quanto evidenziato, tra gli elementi che per legge deve contenere la fattura non figura

il numero di conto corrente del beneficiario della prestazione (art. 21, comma 2, d.P.R. n. 633/1972 e successive modifiche e integrazioni) (*cfr. Nota* del 21 ottobre 2008).

Sistemi di informazione creditizia e dati pubblici

Anche nel 2008 sono diminuiti i reclami e le segnalazioni in materia di trattamento dei dati da parte dei Sistemi di informazione creditizia. La tendenza è riconducibile all'adozione del codice di deontologia di settore (*G.U.* 23 dicembre 2004, n. 300 [doc. *web* n. 1556693]), che risulta sostanzialmente rispettato da parte dei titolari del trattamento.

Sono pervenuti, tuttavia, alcuni reclami e segnalazioni al trattamento, da parte di un sistema di informazione creditizia, di dati personali tratti da pubblici registri e riferiti a pignoramenti e ipoteche nei cui confronti è intervenuta, nelle forme di legge, la cancellazione o altra annotazione, che nei *report* della società che gestisce il sistema risultavano con la sola locuzione sintetica *"atto colpito da annotamento"*.

Il Garante, al riguardo, ha stabilito che la locuzione sintetica *"atto colpito da annotamento"*, non risulta conforme ai princìpi di esattezza e completezza dei dati personali (art. 11, comma 1, lett. *c*) e *d*), del Codice), per il suo contenuto generico e i riflessi negativi sull'interessato (derivanti dal termine *"colpito"*), frutto di elaborazione propria della società che non rappresenta fedelmente e immediatamente quanto contenuto nei registri pubblici. L'art. 10, comma 3, del Codice stabilisce, inoltre, che *"il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare"* (*cfr.* anche *Provv.* 4 maggio 2006, punto 7 [doc. *web* n. 1302311]). Pertanto la società, disponendo di informazioni di dettaglio riguardanti le vicende relative all' *"atto colpito da annotamento"*, deve comunicarle nella loro completezza anche nei riscontri forniti agli interessati, in caso di esercizio del diritto di accesso ai sensi dell'art. 7 del Codice.

Per tali motivi è stato ordinato alla società di sostituire la dizione sintetica *"atto colpito da annotamento"* con informazioni il cui contenuto sia completo e aggiornato rispetto a quello desumibile dai pubblici registri (*Provv.* 5 giugno 2008 [doc. *web* n. 1535726]).