n. 1711492], successivamente pubblicato in *Gazzetta Ufficiale*, nel quale ha in primo luogo ricordato che, nel caso in cui un soggetto attivi una nuova utenza telefonica, fissa o mobile, con un operatore diverso dal precedente indipendentemente dal fatto che il "vecchio" contratto di fornitura sia mantenuto in vita o meno, instaurandosi comunque un nuovo rapporto di fornitura di servizi telefonici, il nuovo operatore, in qualità di titolare del trattamento, è tenuto a sottoporre al cliente il modulo di informativa e raccolta del consenso, di cui all'Allegato IV del *provvedimento* del 2004.

L'Autorità ha inoltre ricordato che, anche nel caso in cui l'interessato, al momento dell'attivazione di una nuova utenza con un operatore diverso, decida di conservare il suo numero telefonico, chiedendo la *number portability* (*Np*) si verifica una modifica nel rapporto di fornitura del servizio, poiché cambia il titolare del trattamento. Pertanto, anche in tale evenienza gli operatori sono tenuti a sottoporre all'attenzione dei propri clienti il modello di informativa e richiesta di consenso.

Tuttavia, in ragione del fatto che nell'ipotesi di *number portability* il numero telefonico non cambia e che, quindi, restano invariati tutti gli elementi oggetto di pubblicazione negli elenchi, il Garante ha ritenuto che i clienti che cambiano operatore con *Np*, possano essere assimilati ai "vecchi" clienti presi in considerazione dal *provvedimento* del 2004, ossia quei soggetti i cui nominativi erano già presenti negli elenchi pubblicati prima dell'entrata in vigore del nuovo regime degli elenchi telefonici.

Anche i predetti soggetti infatti hanno già espresso in passato al proprio operatore la volontà di inserimento nel Dbu e, conseguentemente, negli elenchi, dei dati personali che li riguardano.

Il Garante ha quindi stabilito che, per tali soggetti, il nuovo operatore telefonico possa mantenere invariate le opzioni scelte in passato, in assenza di risposta al suindicato questionario nel termine di sessanta giorni dalla ricezione dello stesso, restando naturalmente la possibilità per i medesimi soggetti di manifestare in qualunque momento una diversa volontà, rivolgendosi anche successivamente al nuovo operatore.

*8.6.4. Banche dati utilizzate per il* telemarketing

A seguito di numerose segnalazioni relative ad attività promozionali effettuate mediante l'invio di materiale cartaceo e contatto telefonico, il Garante ha avviato d'ufficio un'articolata attività istruttoria sull'utilizzo di banche dati per finalità di *marketing.*

Infatti, nonostante gli interventi dell'Autorità (nel corso del 2007 con alcuni p*rovvedimenti* indirizzati a diversi titolari del trattamento [doc. *web* nn. 1412626, 1412610, 1412598, 1412557 e 1412586], *cfr. Relazione 2007*, pag. 83; nel 2008 nei confronti di altri tre soggetti che fornivano alle società telefoniche i *database* utilizzati per campagne di *telemarketing* con altrettanti *provvedimenti* inibitori [doc. *web* nn. 1544315, 1544326, 1544338, 1562780 e 1562758], *cfr. Relazione 2008*, pag. 112) è emerso che il fenomeno del *marketing* indesiderato continua ad assumere un rilievo sempre maggiore.

L'istruttoria aveva preso avvio nel 2008 con una serie di accertamenti ispettivi nei confronti di soggetti che operano nel settore della formazione, gestione e cessione di banche dati e elenchi anagrafici nonché delle altre informazioni utili all'effettuazione di campagne promozionali e che dunque, trattano dati personali per finalità di *marketing* sia in qualità di cedenti che di cessionari di tali *database.*

Modifiche della normativa

Nel corso del 2009 l'utilizzo di dati personali contenuti in banche dati per finalità di *marketing* è stato oggetto di numerosi interventi del legislatore.

Dopo i primi accertamenti ispettivi (settembre 2008–febbraio 2009) è entrata in vigore la disciplina derogatoria e transitoria relativa all'utilizzo delle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005, introdotta dalla legge 27 febbraio 2009, n. 14 (mediante l'emendamento all'art. 44 del d.l. 30 dicembre 2008, n. 207 convertito, con modificazioni, nella citata l., in *G.U.* 28 febbraio 2009, n. 28), sul cui ambito di applicazione il Garante si è espresso con un *provvedimento* di carattere generale adottato il 12 marzo 2009 (*G.U.* 20 marzo 2009, n. 66 [doc. *web* n. 1598808]; *cfr. Relazione 2008*, p.114). I successivi accertamenti ispettivi hanno avuto ad oggetto la verifica della conformità alle prescrizioni contenute in tale *provvedimento.*

Successivamente, l'art. 20-*bis* della legge 20 novembre 2009, n. 166 (*G.U.* 24 novembre 2009, n. 215, con la quale è stato convertito, con modificazioni, il d. l. 25 settembre

2009, n. 135) ha modificato nuovamente la disciplina relativa agli elenchi telefonici, già derogata nei termini di cui sopra.

In particolare, la l. n. 166/2009 ha modificato l'art. 130 del Codice, consentendo il trattamento dei dati tramite contatti telefonici, per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, salvo il diritto di opposizione dell'interessato. La nuova disciplina prevede, quindi, l'istituzione di un "registro pubblico delle opposizioni" entro sei mesi dalla data di entrata in vigore della legge medesima e stabilisce che *"fino al suddetto termine, restano in vigore i provvedimenti adottati dal Garante per la protezione dei dati personali (...) in attuazione dell'articolo 129 del medesimo codice"*.

Alla luce di questo e, in prospettiva dell'attuazione della nuova disciplina, la deroga transitoria e temporanea (che in base al disposto della l. 27 febbraio 2009, n. 14, scadeva il 31 dicembre 2009) è stata prorogata *"sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto legge 25 settembre 2009, n. 135"* (art. 20-*bis*, comma 3, legge 20 novembre 2009, n. 166).

Successivamente a tale modifica legislativa, il Garante ha approvato in data 22 dicembre 2009 un nuovo *provvedimento* ([doc. *web* n. 1683085], in *G.U.* 15 gennaio 2010, n. 11) che ha prorogato l'efficacia del citato *provvedimento* del 12 marzo 2009 sino all'istituzione del predetto registro pubblico delle opposizioni.

Tuttavia occorre rilevare che il nuovo quadro normativo, delineato per esigenze di completezza, dispone per il futuro e dunque ha un impatto limitato sugli esiti dei procedimenti amministrativi relativi alle menzionate società oggetto di ispezione.

Nel complesso, sono state ispezionate dieci società, e redatti venticinque verbali, a ciascuno dei quali sono allegati, mediamente, una decina di documenti anche di carattere tecnico, cui si vanno ad aggiungere i documenti integrativi trasmessi dalle società nei giorni successivi.

L'articolato quadro complessivo emerso dalla totalità delle ispezioni ha evidenziato, in linea generale, un diffuso utilizzo di dati raccolti in violazione delle disposizioni del Codice in materia di informativa e consenso degli interessati.

Tali violazioni hanno determinato l'adozione di ulteriori provvedimenti inibitori e prescrittivi, nonché l'applicazione di sanzioni amministrative per le violazioni previste dal Codice.

In taluni casi, si è resa necessaria la trasmissione degli atti alle competenti procure della Repubblica per l'accertamento di fattispecie di natura penale previste dal Codice (per trattamento illecito dei dati, inosservanza dei provvedimenti dell'Autorità, falsità nelle dichiarazioni al Garante e mancata adozione delle misure minime di sicurezza).

Inoltre, poiché le attività ispettive sono state eseguite durante l'intero arco di tempo in cui il legislatore ha apportato le modifiche al sistema sanzionatorio (dal 1° gennaio 2009), si segnala che l'importo e la natura delle sanzioni amministrative hanno necessariamente tenuto conto della data dell'accertamento.

Per la prima volta, infine, relativamente ad alcune sanzioni amministrative è stata applicata l'aggravante prevista dall'art. 164-*bis*, commi 2 (banche dati di particolare rilevanza o dimensioni) e 3, del Codice, in ragione dell'elevato numero di interessati.

*8.6.5. Attività di profilazione della clientela*

Con un *provvedimento* generale rivolto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico (*Provv.* 25 giugno 2009 [doc. *web* n. 1629107]) l'Autorità ha stabilito i parametri e le misure minime da seguire per il corretto trattamento dei dati personali dei clienti per finalità di profilazione.

Da un'articolata e complessa attività istruttoria, anche di carattere ispettivo, rivolta a diversi operatori del settore allo scopo di individuare le modalità di svolgimento dell'attività di profilazione della clientela, era emerso che il trattamento di dati personali da parte dei gestori telefonici, diretto ad individuare abitudini di consumo, preferenze e spese telefoniche dei clienti, veniva in molti casi effettuato senza acquisirne il preventivo consenso e senza fornire un'idonea informativa.

L'Autorità è intervenuta per ribadire, in primo luogo, che i dati personali non possono essere utilizzati per tali finalità in assenza di un'adeguata informativa e di un espresso consenso dei soggetti interessati.

Il Garante ha altresì chiarito che le stesse regole operano, in generale, anche con riguardo all'attività di profilazione svolta attraverso dati personali aggregati, i quali non possono, per ciò solo, definirsi come dati anonimi, traendo origine da dati personali presenti in forma completa e dettagliata in una pluralità di sistemi originari che restano nella disponibilità del titolare del trattamento per altre esigenze e finalità ed ai quali è possibile risalire. In tali casi il trattamento può presentare rischi specifici per i diritti e le libertà fondamentali degli utenti, da valutarsi in base alla profondità del livello di aggregazione effettuato dal titolare e alle modalità tecniche utilizzate.

L'Autorità ha tuttavia previsto, per l'attività di profilazione effettuata con l'ausilio di dati aggregati dei clienti di cui non era risultato acquisito il consenso, la possibilità per i fornitori di presentare un'istanza di verifica preliminare, con l'indicazione delle finalità e tipologia dei dati da utilizzare, spettando al Garante valutare, caso per caso, se consentire il trattamento senza l'esplicito consenso degli interessati, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice. Ciò in quanto, l'attività di profilazione rappresenta una delle attività prevalenti degli operatori del settore che vi ricorrono per supportare i propri processi decisionali e strategici.

Entro il termine del 30 settembre 2009, stabilito dall'Autorità per formulare le istanze di *prior checking*, sono pervenute all'Ufficio diverse richieste, in particolare dai sette maggiori gestori di telefonia presenti sul mercato. E' stata perciò condotta un'approfondita istruttoria per ogni singolo operatore, per verificare la sussistenza dei parametri e delle condizioni individuate con il *provvedimento* generale e, conseguentemente l'opportunità di autorizzare il trattamento o di prescrivere eventuali misure specifiche, e i tempi per attuare le prescrizioni indicate.

L'esito di tale attività, che ha comportato un'analisi dettagliata dei sistemi informatici aziendali deputati alla profilazione, anche rispetto alle piattaforme gestionali e agli apparati di rete dei diversi gestori telefonici, ha evidenziato la necessità di emanare una serie di prescrizioni, attraverso *provvedimenti* inviati a ciascun gestore.

Queste ultime hanno riguardato il livello di aggregazione e la tipologia dei dati utilizzati, la separazione funzionale dei sistemi dedicati alla profilazione rispetto a quelli

utilizzati per altre finalità aziendali, come quelle di *marketing*, nonché i processi di mascheramento dei dati personali aggregati, utilizzati per profilare la clientela.

L'Autorità ha inoltre prescritto l'adozione di alcune misure nelle procedure di autenticazione e autorizzazione degli addetti all'attività in parola, individuando un periodo massimo di conservazione dei dati utilizzati, e, al contempo, ordinandone la cancellazione, ovvero la trasformazione irreversibile in forma anonima, alla relativa scadenza.

Ulteriori misure sono state impartite per la revisione dell'informativa da rendere agli interessati ai sensi dell'art. 13 del Codice, con riguardo al trattamento svolto attraverso dati aggregati, nonché per la necessaria notificazione del trattamento ai sensi degli artt. 37, comma 1, lett. *d*), e 38 del Codice.

In ragione della complessità delle misure tecniche previste e delle modifiche da apportare ai sistemi coinvolti nella profilazione, attraverso dati personali aggregati, l'Autorità ha previsto, per l'adozione degli adempimenti prescritti, un termine variabile tra i trenta ed i centottanta giorni.

Con riguardo, invece, all'attività svolta attraverso l'uso di dati personali individuali dei clienti, l'Autorità ha ribadito l'esigenza di acquisire il consenso preventivo, libero e specifico dell'interessato.

In questo ambito, con particolare riguardo alla corretta applicazione degli artt. 13 e 23 del Codice, si ricorda il *provvedimento*, emanato dall'Autorità in materia di *"fidelity card"*, del 24 febbraio 2005 [doc. *web* n. 1103045], nel quale veniva evidenziata la necessità che il cliente fosse messo in grado di manifestare un consenso libero e specifico rispetto a ciascun trattamento di dati chiaramente individuato (art. 23, comma 3), ossia un consenso differenziato per le diverse attività di profilazione e di *marketing* svolte nell'ambito dei servizi di comunicazione elettronica accessibili al pubblico.

## 9. PROPAGANDA ELETTORALE E ASSOCIAZIONI

Trattamento di dati per finalità di propaganda elettorale

Anche nel 2010 il Garante, in vista delle consultazioni elettorali di marzo-aprile, ha in via temporanea (*Provv.* 11 febbraio 2010, in *G.U.* 22 febbraio 2010, n. 43 [doc. *web* n. 1694531]) esonerato dall'obbligo di informativa - di cui all'art. 13 del Codice - partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati che trattano dati personali per esclusiva finalità di selezione di candidati alle elezioni, di comunicazione politica o di propaganda elettorale.

I suddetti soggetti sono stati esonerati dal rendere l'informativa fino al 30 maggio 2010; decorsa tale data, essi possono continuare a trattare temporaneamente (anche mediante mera conservazione) i dati personali lecitamente raccolti secondo le modalità indicate nel *provvedimento* generale del 7 settembre 2005 (*G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613]), le cui prescrizioni sono state a tal fine integralmente richiamate. Ciò sempreché informino gli interessati entro il 31 luglio 2010, nei modi previsti dal Codice.

Dai predetti *provvedimenti* emergono ulteriori princìpi che devono essere osservati dai soggetti 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 *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. Le medesime cautele devono essere osservate anche laddove il terzo, oltre a fornire i dati, svolga le funzioni di responsabile del trattamento designato da chi effettua la propaganda.

Per quanto riguarda la casistica, è da menzionare che l'Autorità è stata interpellata dal Comune dell'Aquila a proposito delle richieste pervenute da parte delle forze politiche di acquisire, a fini di propaganda elettorale, gli elenchi in cui a seguito del sisma del 2009 sono stati registrati i nuovi indirizzi provvisori degli elettori. Tali recapiti, privi dei riferimenti telefonici, sono raccolti dal Comune medesimo in apposite banche dati, correlate alle diverse tipologie di "modalità abitative" (Moduli abitativi provvisori, Moduli

abitativi rimovibili, Progetto "Case", affitti concordati, strutture ricettive, autonoma sistemazione all'interno e al di fuori del territorio aquilano), al fine di controllare il movimento migratorio tuttora in atto.

Al riguardo, in relazione ai soli profili di competenza del Garante, non è stata ritenuta preclusa, con riferimento alle specifiche esigenze rappresentate con il quesito, la possibilità che per l'inoltro di messaggi elettorali e politici possano essere fornite, ai richiedenti legittimati, gli indirizzi provvisori dei soli cittadini iscritti nelle liste elettorali in possesso del Comune dell'Aquila, con esclusione di ogni altra informazione non pertinente (*Provv.* 4 febbraio 2010 [doc. *web* n. 1694777]).

Il provvedimento è stato trasmesso al Ministero dell'interno, per le valutazioni di competenza in relazione alle specifiche disposizioni di settore applicabili (*Nota* 11 febbraio 2010).

In un altro caso, una società aveva posto un quesito sulla possibilità di acquisire presso i comuni copia delle liste elettorali per conto di partiti, organismi politici, comitati e singoli candidati, i quali si erano rivolti alla società medesima per ottenere servizi di imbustamento, stampa e recapito, tramite il servizio postale, di comunicazioni di propaganda elettorale, comprensivi anche della gestione dei dati personali (nominativi e indirizzo) dei destinatari delle comunicazioni.

In proposito si è preso atto che i predetti soggetti, anche in maniera coordinata tra loro, nella loro qualità di titolari del trattamento dei dati contenuti nelle liste elettorali, avevano commissionato alla società, designandola a tale fine responsabile del trattamento (art. 29 del Codice), lo svolgimento delle operazioni di trattamento per la campagna elettorale e, inoltre, che la società aveva espressamente escluso la possibilità di perseguire proprie finalità autonome quale titolare del trattamento, in specie, di commercializzazione dei dati così raccolti per servizi di *marketing* diretto.

E' stato puntualizzato, comunque, che l'eventuale acquisizione dei dati personali da un soggetto 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 dall'onere di verificare, anche

con modalità a campione e avvalendosi del mandatario elettorale, che il terzo: a) abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda elettorale e abbia ottenuto il loro consenso idoneo ed esplicito; il consenso deve risultare manifestato liberamente, in termini differenziati rispetto all'eventuale prestazione di beni e servizi e documentato per iscritto; b) non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili (artt. 11 e 61 del Codice).

In ultimo, non è stato ritenuto corretto il trattamento dei dati personali che la società intendeva effettuare a seguito della raccolta e dell'archiviazione elettronica delle liste acquisite nella qualità di responsabile del trattamento: è stato sottolineato come non risulti lecito rendere utilizzabili i dati personali così acquisiti e detenuti nei confronti di altri partiti, candidati ed organismi che ne facciano successivamente richiesta (*Nota* 24 febbraio 2010).

Associazioni

L'Autorità è stata chiamata a definire un reclamo in merito al trattamento di dati personali svolto presso un'associazione avente lo scopo di promuovere azioni di evangelizzazione e di apostolato verso individui ammalati e disabili (*Provv.* 2 aprile 2009 [doc. *web* n. 1606059]).

La reclamante, in qualità di ex associata, aveva lamentato la ricezione di una lettera dal contenuto propagandistico-elettorale inviata da un componente del consiglio direttivo dell'associazione, che avrebbe a tal fine utilizzato alcuni suoi dati personali, oltre a quelli di altri iscritti.

A seguito delle verifiche effettuate, anche di tipo ispettivo, l'Autorità ha ritenuto il trattamento dei dati personali della reclamante effettuato per finalità non compatibili con gli scopi originari della raccolta, con conseguente violazione dell'art. 11, comma 1, lett. *a*) e *b*), del Codice. Inoltre, non è risultato comprovato che fosse stata resa l'informativa all'interessata e acquisito il relativo consenso anche per finalità di propaganda elettorale.

Peraltro, in considerazione della natura dell'associazione e dei dati trattati, idonei a rivelare anche le convinzioni religiose degli interessati, l'associazione avrebbe dovuto adottare idonee e preventive misure di sicurezza, anche per prevenire eventuali rischi

di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le risultanze istruttorie hanno invece evidenziato la mancata adozione, all'epoca dei fatti contestati, di tali misure.

In particolare, non è risultato provato che l'associazione avesse all'epoca designato gli incaricati per il trattamento dei dati personali riferiti agli associati (né tale era il componente del consiglio direttivo coinvolto nella vicenda), né che avesse provveduto ad adeguati interventi formativi sul personale addetto alle operazioni di trattamento dei dati degli aderenti.

L'Autorità al riguardo ha prescritto all'associazione di adottare, in relazione all'archivio, le misure di sicurezza previste dagli artt. 31 *ss.* del Codice, e di utilizzare le informazioni contenute nell'archivio esclusivamente per finalità storiche e statistiche; è stato inoltre prescritto all'associazione di provvedere alla designazione degli incaricati del trattamento. L'Autorità ha peraltro inviato gli atti alla Procura della Repubblica per l'eventuale contestazione del reato di cui all'art. 169 del Codice.

# 10. LE ATTIVITÀ ECONOMICHE E I RAPPORTI DI LAVORO

## 10.1. SETTORE BANCARIO

Come già registrato nelle precedenti edizioni, anche nel 2009 la materia bancaria è stata oggetto di numerosi interventi dell'Autorità tesi, oltre che a ribadire l'esigenza di adottare le misure minime di sicurezza, a prescrivere il rigoroso controllo sull'attività degli incaricati nonché a sensibilizzare gli stessi al rispetto delle istruzioni ricevute.

In particolare, con una segnalazione l'interessata aveva lamentato, nell'ambito di una causa di separazione, il deposito di una memoria difensiva nell'interesse del marito, contenente informazioni bancarie a sé riferite ed asseritamente acquisite tramite un funzionario della banca.

Nell'ambito dei controlli svolti dall'Autorità, è emerso che effettivamente un dipendente della banca aveva effettuato alcune interrogazioni sui conti correnti bancari della segnalante, dando comunicazione degli esiti ad altro dipendente appartenente a una società dello stesso gruppo bancario e che detti accessi erano stati effettuati da una filiale diversa da quella nella quale il conto corrente risultava acceso.

Il Garante, con *provvedimento* del 18 giugno 2009 [doc. *web* n. 1635720], ha dichiarato illecito il trattamento di dati personali effettuato presso l'istituto di credito nelle forme della consultazione e della loro successiva comunicazione a terzi (nel caso di specie, altro dipendente dello stesso gruppo bancario) ed ha altresì prescritto al titolare del trattamento di adottare le misure di sicurezza "idonee" ad evitare accessi non autorizzati e tese a garantire la scrupolosa vigilanza sull'operato degli incaricati, nonché a sensibilizzare gli stessi incaricati al rispetto delle istruzioni ricevute anche nel corso delle iniziative formative (regola 19.6. dell'Allegato B. al Codice).

In un altro caso, la segnalante aveva lamentato una comunicazione a terzi di dati bancari a sé riferiti, successivamente utilizzati nell'ambito di un procedimento di pignoramento presso terzi. Nel corso degli accertamenti effettuati, sono stati riscontrati accessi indebiti compiuti da un terminale posto presso una filiale della banca presso la quale la segnalante era stata correntista, ma dove aveva successivamente estinto tale conto.

Tale trattamento illecito era stato peraltro possibile anche grazie all'utilizzo di una postazione erroneamente configurata (che consentiva anche a livello di filiale la visualizzazione di informazioni relative alla clientela prevista per unità organizzative di "area territoriale"): ciò in violazione degli artt. 3, 31 *ss.* del Codice, che prescrivono misure organizzative e di sicurezza finalizzate alla riduzione di accessi non autorizzati o non conformi alle finalità del trattamento.

Anche in questo caso, ritenuto che la banca avesse adottato le misure di sicurezza "minime" a protezione dei dati dei clienti trattati con l'ausilio di strumenti elettronici conformi a quanto prescritto dagli artt. 33 e 34 del Codice e dalle regole 1-26 dell'Allegato B. al Codice, il Garante ha tuttavia prescritto alla banca di adottare idonee misure organizzative, ai sensi dell'art. 31 del Codice, tese sia a garantire la scrupolosa vigilanza sull'operato degli incaricati, sia a sensibilizzare gli incaricati al rispetto delle istruzioni ricevute (*Provv.* 23 luglio 2009 [doc. *web* n. 1640294]).

In un'altra fattispecie il segnalante - socio accomandatario di una società presso la quale collaborava anche il figlio - aveva lamentato che una società emittente carte di credito, nell'ambito di un procedimento di separazione giudiziale relativa al nominato figlio, avesse dato esecuzione ad una pronuncia dell'autorità giudiziaria contenente la richiesta rivolta alla Guardia di finanza di accertare se il figlio avesse la disponibilità delle carte di credito della società, se ne avesse fatto e ne facesse utilizzo e con quale frequenza, per quali spese e per quali importi. In particolare, il segnalante aveva lamentato che la società emittente carte di credito avesse comunicato anche dati inerenti ad operazioni riferite ad una carta non intestata al figlio.

L'Autorità, pur tenendo conto delle peculiari circostanze riferite dal titolare del trattamento che avevano reso possibile l'indebita comunicazione di informazioni non pertinenti rispetto alla controversia pendente (art. 11 del Codice) e che tale trattamento aveva esaurito i suoi effetti (fatta salva ogni valutazione dell'autorità giudiziaria adita circa l'ammissibilità e la rilevanza delle prove acquisite in corso di causa) ha ritenuto di dover richiamare in ogni caso l'attenzione della società sulla necessità di una più rigorosa vigilanza sull'operato degli incaricati e sul rispetto e l'attuazione da parte dei medesimi

delle istruzioni loro impartite (*Nota* 4 dicembre 2009).

In un altro reclamo è stata lamentata l'illecita comunicazione a terzi, nella specie al padre del segnalante, di informazioni bancarie riferite al figlio. In particolare il genitore, convocato presso l'istituto bancario per il tramite della polizia municipale, era stato messo a conoscenza di una grave situazione debitoria in capo al figlio, con l'indicazione delle cifre di scoperto e del dettaglio di tutti i movimenti del conto corrente.

All'esito dell'attività istruttoria il Garante, con *provvedimento* del 28 maggio 2009 [doc. *web* n. 1624734] ha ritenuto che il comportamento tenuto dal personale della banca avesse determinato un trattamento di dati personali non previamente autorizzato dall'interessato (art. 23 del Codice) non conforme a correttezza (art. 11, comma 1, lett. *a*), del Codice). La banca, una volta acquisito il recapito telefonico dell'interessato, avrebbe dovuto mettersi in contatto solo con il figlio, e rimettere ad un'autonoma scelta di questo le successive iniziative da assumere.

Il Garante ha, inoltre, ritenuto che le modalità utilizzate dalla banca per prendere contatto con il padre del segnalante attraverso la polizia municipale fossero in violazione dell'art. 11, comma 1, lett. *a*), del Codice dal punto di vista della correttezza del trattamento, essendo per sé idonee a rendere edotti soggetti terzi (privi di titolo alcuno per operare quali ausiliari della banca) delle relazioni bancarie tra padre e figlio.

In un reclamo una società aveva rappresentato che, a seguito della cessazione dalla carica di un procuratore, aveva richiesto al proprio istituto bancario di disattivare le credenziali di autenticazione a lui assegnate per accedere *online* ai conti bancari societari. La banca tuttavia, nonostante i numerosi successivi solleciti, non aveva dato seguito alla richiesta, comunicando con ritardo l'avvenuta revoca delle credenziali del procuratore. All'esito degli accertamenti ispettivi svolti dall'Autorità il ritardo è risultato addebitabile a un errore del personale dell'agenzia. Il Garante ha pertanto richiamato la banca ad adottare le misure di sicurezza idonee a contenere il rischio di accesso non autorizzato ai sensi dell'art. 31 del Codice, ossia ad assicurare la tempestiva disattivazione delle credenziali di autenticazione attribuite alla clientela (*Provv.* 28 maggio 2009 [doc. *web* n. 1624668]).

Un segnalante aveva lamentato, da parte di una banca, l'illecita comunicazione di informazioni riguardanti suoi rapporti bancari al legale della sua controparte, che le avrebbe successivamente utilizzate nell'ambito di un procedimento giudiziario.

All'esito dell'attività istruttoria, con *nota* del 4 aprile 2009, il Garante ha rilevato in via preliminare che l'art. 160, comma 6, del Codice (in conformità, dal punto di vista sistematico, all'art. 116, primo comma c.p.c.) prevede che la valutazione della validità, efficacia e utilizzabilità di atti e documenti nell'ambito del procedimento giudiziario basati sull'illegittimo trattamento di dati personali spettano all'autorità giudiziaria.

Con specifico riferimento al caso in esame, il Garante ha ritenuto non comprovata una violazione della disciplina in materia di protezione dei dati personali - non risultando illecita la comunicazione - quando il terzo citato nell'ambito di una procedura di sequestro conservativo (nel caso di specie, la banca) rende la dichiarazione nei modi previsti dall'art. 547 c.p.c., come modificato dalla legge 24 febbraio 2006, n. 52 (*Riforma delle esecuzioni mobiliari*), tra cui rientra la comunicazione con invio di raccomandata.

**Fusioni e scissioni**

Considerata la ricorrenza delle operazioni societarie di fusione e di scissione e del connesso trattamento di dati personali dei soggetti interessati coinvolti, il Garante ha adottato l'8 aprile 2009 un *provvedimento* di carattere generale [doc. *web* n. 1609999] nel quale ha fornito chiarimenti circa gli adempimenti che devono essere posti in essere per rendere il trattamento conforme alla disciplina di protezione dei dati personali.

Il provvedimento, conforme alle decisioni adottate in materia nei confronti di due istituti di credito (*Provv.* 11 dicembre 2008 [doc. *web* n. 1584328] e *Provv.* 19 dicembre 2008 [doc. *web* n. 1584272]), ha stabilito che, a seguito del processo di fusione o scissione, le società coinvolte devono informare tutti i soggetti interessati (clienti, lavoratori, fornitori, *ecc.*) su chi sia il titolare e il nuovo responsabile del trattamento dei dati personali in possesso dell'impresa, al quale potersi rivolgere per esercitare il diritto di accesso e tutti gli altri diritti previsti dal Codice.

La soluzione della *"continuità"* tra i soggetti interessati dalla fusione è conforme a quella seguita dalle Sezioni unite della Corte di Cassazione (sentenza n. 2637 dell'8 febbraio 2006), in base alla quale *"la fusione tra società, prevista dagli artt. 2501 c.c. e segg.,*

*non determina, nella ipotesi di fusione per incorporazione, l'estinzione della società incorporata, né crea un nuovo soggetto di diritto nell'ipotesi di fusione paritaria; ma attua l'unificazione mediante l'integrazione reciproca delle società partecipanti alla fusione. Il fenomeno non comporta, dunque, l'estinzione di un soggetto e (correlativamente) la creazione di un diverso soggetto, risolvendosi [...] in una vicenda meramente evolutiva-modificativa dello stesso soggetto, che conserva la propria identità, pur in un nuovo assetto organizzativo".*

Per semplificare gli adempimenti nella fase di cambiamento societario, l'Autorità ha altresì prescritto, quale misura opportuna, l'aggiornamento dell'informativa resa dalla società scissa e dalle società partecipanti alla fusione (in particolare: la nuova denominazione del titolare del trattamento, gli estremi identificativi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali) attraverso il sito *web* delle società interessate dalle operazioni di scissione e fusione e, con comunicazione individualizzata agli interessati, in occasione della prima circostanza utile di contatto.

Nel caso in cui le società risultanti dal processo di fusione o scissione effettuino trattamenti in cui è prevista la notificazione al Garante, tali aziende dovranno effettuare o integrare la notificazione secondo le procedure *standard* previste dall'Autorità.

Comunicazioni infragruppo tra intermediari finanziari

Il Garante, a seguito di un quesito pervenuto, ha adottato il 10 settembre 2009 un *provvedimento* [doc. *web* n. 1664492] relativo alla comunicazione, tra intermediari finanziari appartenenti ad un medesimo gruppo, di dati personali relativi alle segnalazioni di operazioni considerate "sospette" ai sensi della normativa antiriciclaggio.

In particolare, all'Autorità era stato chiesto di valutare la ricorrenza, in relazione a dette comunicazioni (ivi comprese quelle verso intermediari appartenenti allo stesso gruppo stabiliti in Paesi terzi), dei presupposti per l'applicazione dell'art. 24, comma 1, lett. *g*) del Codice (relativo al *cd.* "bilanciamento di interessi").

Al riguardo occorre ricordare che sulla questione del coordinamento tra la normativa sulla protezione dei dati personali e la disciplina in materia di antiriciclaggio il Garante si era già espresso con il *parere* del 25 luglio 2007 [doc. *web* n. 1431012].

Nel *provvedimento* del 2009 il Garante ha ritenuto che, nel caso di specie, vi fossero