eventualmente con quali dati (ad. es., solo con il cognome e l'iniziale del nome). Il secondo modello é relativo ai vecchi abbonati e dovrà essere inviato alla prima occasione utile di contatto (rendiconti, fatture, altre comunicazioni di servizio) oltre che essere inserito nei siti *web* degli operatori. Il modello dovrà specificare che l'abbonato ha sempre diritto di cancellarsi in ogni momento dagli elenchi telefonici.

Si evidenzia che il mancato rispetto delle prescrizioni del Garante comporterà sanzioni amministrative da un minimo di 30.000 ad un massimo di 180.000 euro, che potranno raggiungere, nei casi di violazione più grave, i 300.000 euro.

Obbligo di rendere l'informativa con riguardo alla raccolta dei dati presso terzi

Con riguardo all'obbligo di rendere l'informativa, quando i dati non sono raccolti presso l'interessato, all'atto della registrazione degli stessi o al più tardi, quando ne è prevista la comunicazione, non oltre la prima comunicazione (art. 13, comma 4, del Codice), l'Autorità ha ricevuto diverse istanze di esonero ai sensi dell'art. 13, comma 5, lett. *c*), del Codice e di conseguente individuazione di modalità equipollenti per informare gli interessati qualora l'informativa in forma individualizzata comporti un impiego di mezzi che il Garante dichiari manifestamente sproporzionato rispetto al diritto tutelato.

L'Autorità ha, in ragione delle diverse fattispecie esaminate, assunto differenti determinazioni. In alcuni casi ha respinto l'istanza di esonero, in particolare, con riguardo a dati estratti dal DBU (*database* telefonico unico), in ragione del fatto che i trattamenti che il titolare intendeva svolgere con l'ausilio di tali dati esulavano dalle finalità per le quali detto *database* è stato costituito. Il Garante ha infatti ribadito che il DBU rappresenta un archivio elettronico unico, contenente i dati personali dei clienti di tutti gli operatori di telefonia fissa e mobile per la formazione degli elenchi telefonici e la fornitura dei servizi di informazione abbonati, e pertanto non può essere utilizzato per finalità diverse da quelle per le quali è stato costituito se non in violazione dell'art. 11, comma 1, lett. *b*), del Codice (*Provv.* 16 settembre 2010 [doc. *web* n. 1753351]).

Con specifico riguardo all'offerta di servizi integrati di *mailing* postale per finalità di comunicazione commerciale e di *marketing*, è infatti emerso che diverse società, pur raccogliendo i dati presso terzi, non avevano fornito agli interessati l'informativa né al momento della registrazione, né al momento della prima comunicazione così come stabilito dal cit.

art. 13, comma 4 del Codice, essendo invalsa la prassi di rendere l'informativa con il primo *mailing* postale inviato per conto dei propri clienti o direttamente da questi ultimi. A fronte dei provvedimenti emanati dall'Autorità che hanno vietato il trattamento in assenza dell'informativa, prevista dall'art. 13, comma 4, del Codice, sono successivamente pervenute al Garante istanze di esonero ai sensi del successivo comma 5, lett. *b*), della norma. L'Autorità ha valutato la sussistenza dei presupposti per disporre l'esonero (la sproporzione dei mezzi, con riguardo sia all'elevato numero di interessati, operatori economici ed istituzionali, sia all'onerosità di tali mezzi) e previsto l'adozione di misure alternative per consentire di rilasciare agli interessati un'adeguata informativa generale, con modalità idonee e di facile accesso. Ciò sia nel caso in cui i dati personali siano stati acquisiti direttamente da fonti pubblicamente accessibili, sia nel caso in cui siano stati forniti da società specializzate. Il Garante ha anche previsto, nel caso di cessione dei dati, un'integrazione dell'informativa rilasciata con il primo contatto commerciale con alcune specifiche informazioni, proprio in ragione dell'informativa generale rilasciata precedentemente ai sensi dell'art. 13, comma 5, lett. *b*), del Codice (*Provv.* 16 dicembre 2010 [doc. *web* n. 1781973]).

9.7. USO DELLA TECNOLOGIA *RFID* NELLE TESSERE *SKI-PASS*

L'Autorità ha affrontato anche il complesso tema dell'uso dei dati personali attraverso la tecnologia *RFID* (*Radio Frequency Identification*), in particolare con riguardo all'utilizzo di tessere *ski-pass* per l'accesso agli impianti sciistici di un vasto comprensorio sciistico del Nord Italia.

L'intervento ha fatto seguito ad una serie di accertamenti ispettivi, svolti dal Nucleo speciale *privacy* della Guardia di finanza, presso i gestori degli impianti sciistici per verificare il rispetto della normativa sulla protezione dei dati personali, soprattutto con riguardo alle modalità e finalità della raccolta dei dati personali degli sciatori, al rispetto degli obblighi di informativa, nonché degli obblighi di notificazione e di eventuale acquisizione del consenso degli interessati.

In particolare, il problema della notificazione del trattamento è stato esaminato alla luce dall'art. 37, comma 1, lett. *a*), del Codice rispetto al trattamento di dati che indicano la

posizione geografica di persone mediante una rete di comunicazione elettronica, oltre che del *provvedimento* 9 marzo 2005 sulle *cd.* "*etichette intelligenti*" [doc. *web* n. 1109493].

Le società che gestiscono impianti di risalita utilizzano infatti la tecnologia *RFID*, integrata nei *badge* che gli sciatori usano per l'apertura automatica dei tornelli di accesso agli impianti di risalita, al fine di agevolarne i transiti.

In ragione del rilascio anche di tessere nominative è stata verificata la possibilità di individuare la posizione geografica dello *ski-pass* (*cd.* "*geolocalizzazione*") e di ricostruire il percorso effettuato dall'utente nell'ambito del comprensorio sciistico, circostanza che implica l'obbligo di notificazione del trattamento al Garante ai sensi del citato art. 37, comma 1, lett. *a*), del Codice.

All'esito di un esame approfondito, anche nei profili tecnici, è emerso che il ricorso alla tecnologia *RFID* da parte dei gestori degli impianti consente attualmente solo di registrare l'ingresso dello sciatore all'impianto di risalita e che i *chip RFID* vengono attivati esclusivamente al varco di accesso con un raggio di azione di pochi centimetri, senza possibilità di lettura a distanza e di conseguente localizzazione del soggetto. Il problema di una possibile ricostruzione del percorso sciistico effettuato dagli utenti e della sussistenza di un conseguente obbligo di notificazione al Garante è emerso anche con riguardo ad un ulteriore servizio, fornito da alcuni gestori, attraverso l'uso di una carta *RFID* ricaricabile che consente al titolare di visualizzare, attraverso una consultazione *online*, il numero degli impianti utilizzati, il dislivello e la stima dei chilometri di pista percorsi. Anche in tal caso l'Autorità ha accuratamente verificato che i dati raccolti ed utilizzati per fornire il servizio non consentano l'individuazione del percorso dello sciatore, appurando altresì che il servizio, nella sostanza, consente al titolare della carta un accesso diretto, tramite Internet, ai propri dati personali.

Un ulteriore aspetto, oggetto di analisi da parte del Garante, ha riguardato l'obbligo di fornire l'informativa in merito all'utilizzo della tecnologia *RFID*, così come disposto dal citato *provvedimento* 9 marzo 2005, il quale prevede espressamente, in linea con l'orientamento europeo tuttora vigente, che il titolare del trattamento, nel fornire agli interessati l'informativa di cui all'art. 13 del Codice, deve indicare, oltre alle finalità e

modalità del trattamento, anche la presenza di etichette *RFID*, senza che gli interessati si attivino a riguardo.

In proposito, occorre altresì dare evidenza alla presenza di lettori che attivano l'etichetta; l'informativa può essere fornita anche attraverso appositi avvisi agevolmente visionabili per formato e posizionamento, nei luoghi in cui le etichette *RFID* sono utilizzate, ed in tal senso hanno già provveduto diversi gestori di impianti sciistici.

In questo quadro, l'Autorità ha fornito chiarimenti ad una società, indicando anche le misure necessarie per proteggere la riservatezza dell'utente, relativamente al trattamento di dati personali attraverso il servizio "*Ski performance card*", che consente di visualizzare dati relativi alle prestazioni sportive dello sciatore, previo inserimento di un codice univocamente associato al *tag RFID* presente nel relativo *ski-pass* (*Note* 15 e 21 dicembre 2010).

9.8. TRATTAMENTO DEI DATI PERSONALI NEL SETTORE DELLE TELECOMUNICAZIONI

Attivazione di servizi telefonici non richiesti

Diverse segnalazioni di utenti, lamentavano, a fronte dell'attivazione di contratti di abbonamento a servizi di telefonia non richiesti, il rifiuto da parte dei gestori telefonici di fornire la registrazione della conversazione telefonica intercorsa con l'operatore nel corso della quale viene acquisito il consenso all'attivazione del servizio (*cd.* "*verbal ordering*"). Ribadendo il proprio precedente orientamento il Garante (cfr. *Provv.* 8 luglio 2009 [doc. *web* n. 1638561]) ha stabilito che il diritto di accesso ai dati personali dell'interessato, contenuti nella registrazione telefonica, esercitato ai sensi dell'art. 7 del Codice, implica il dovere del titolare di mettere a disposizione copia della stessa al fine di consentire l'acquisizione del dato vocale in essa contenuto (*Note* 24 giugno e 7 luglio 2010).

Invio di comunicazioni commerciali non sollecitate (*spam*)

Anche nel 2010 il Garante ha ricevuto numerose richieste d'intervento relative ad attività di *spam* realizzata mediante diversi mezzi (posta elettronica, fax, chiamate telefoniche, *Sms*).

Rispetto all'anno precedente appaiono in leggera diminuzione le segnalazioni riguardanti la ricezione di fax indesiderati (soprattutto a partire dalla seconda metà dell'anno), anche in ragione degli interventi prescrittivi e sanzionatori effettuati nei confronti degli operatori telefonici (che risultavano essere i maggiori committenti di tale forma di promozione).

Il fax e l'e-mail restano comunque i mezzi più utilizzati per le attività di *spam* anche se, nel corso del 2010, si è notato un leggero incremento delle segnalazioni riguardanti la ricezione di *Sms* e telefonate pre-registrate, che può essere in parte collegato alle campagne elettorali svolte nel corso dell'anno.

Per quanto riguarda il contrasto allo *spam*, molti segnalanti hanno osservato una sensibile diminuzione dei contatti indesiderati a seguito dell'intervento del Garante; persistono, dall'altro lato, le violazioni soprattutto via e-mail, che rendono a volte difficile individuare il titolare del trattamento, per le modalità con cui si può operare in rete e perché spesso i titolari risultano avere sede in Paesi extraeuropei.

L'intervento dell'Autorità nel corso dell'anno è stato più incisivo soprattutto per quanto riguarda i provvedimenti emessi –pressoché raddoppiati rispetto all'anno precedente– e volti prevalentemente a contrastare il fenomeno dello *spam* via e-mail e, in misura maggiore, via fax.

In più occasioni, è stato vietato l'invio, mediante posta elettronica, di comunicazioni promozionali a terzi in assenza di informativa e consenso preventivo e specifico degli interessati ai sensi degli artt. 13 e 130 del Codice (*Provv.* 26 marzo 2010 [doc. *web* n. 1727662]; *Provv.* 8 aprile 2010 [doc. *web* n. 1721205]; *Provv.* 23 settembre 2010 [doc. *web* n. 1758527]).

Il Garante si è occupato anche del diffuso fenomeno dell'invio di fax pubblicitari a destinatari che non avevano mai ricevuto l'informativa né prestato il consenso, intervenendo con diversi provvedimenti inibitori e prescrittivi, accompagnati dall'emanazione delle conseguenti sanzioni amministrative (v. *provvedimenti* 26 marzo 2010 [doc. *web* nn. 1719901 e 1719891]; *Provv.* 6 maggio 2010 [doc. *web* n. 1729175]; *Provv.* 13 maggio 2010 [doc. *web* n. 1737799]; *Provv.* 3 giugno 2010 [doc. *web* n. 1738039]; *provvedimenti* 1 luglio 2010 [doc. *web* nn. 1737773 e 1738592]; *Provv.* 10 novembre 2010 [doc. *web* n. 1769487]; *Provv.* 26 gennaio 2011 [doc. *web* n. 1790365]; *Provv.* 3 febbraio 2011 [doc. *web* n. 1792588]).

In alcuni degli interventi, il Garante ha ricordato che quest'obbligo non può essere eluso inviando un primo messaggio che, nel richiedere il consenso, abbia già un contenuto promozionale (v. *Provv.* 29 maggio 2003, relativo allo *spamming* [doc. *web* n. 29840]).

Nell'occasione, è stato inoltre ribadito che la reperibilità dei dati sugli elenchi pubblici quali, ad esempio gli elenchi categorici, e il trattamento per lo svolgimento di attività economiche non consentono l'esonero previsto dall'art. 24, comma 1, lett. *d*), del Codice, e quindi non esimono il titolare del trattamento, in ragione della specificità del mezzo considerato, dal chiedere il consenso all'interessato per l'uso promozionale del telefax in considerazione della specifica disciplina prevista all'art. 130 del Codice.

Sempre in materia di *spam*, il Garante ha adottato diversi provvedimenti inibitori e prescrittivi anche nei confronti di società che, presumendo di poter inviare comunicazioni pubblicitarie in ragione dell'acquisto da terzi di *database*, non sono state in grado di fornire la documentazione attestante la manifestazione del consenso dei segnalanti al trattamento dei dati personali per finalità di ricezione di messaggi promozionali; in particolare è stato ribadito che, come previsto dal *provvedimento* 29 maggio 2003, relativo allo *spamming* cit., l'utilizzo di dati presenti in banche dati acquistate da terzi, nel caso di invio di comunicazioni automatizzate, deve essere preceduto da apposite verifiche da parte di chi acquista la banca dati stessa, per accertare l'espressione di consensi specifici ed informati degli interessati.

Più in generale, per l'attività di inoltro tramite sistemi automatizzati di messaggi promozionali in modo non sistematico, l'Autorità ha inviato apposite note di richiamo al pieno rispetto della disciplina in materia.

Spam proveniente dall'estero

L'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei: in diversi Paesi infatti la disciplina sulla protezione dei dati personali non garantisce le persone giuridiche.

Si è al riguardo richiesto l'inserimento del Garante nel sistema *CPC* (*Consumer Protection and Cooperation*) istituito dal Regolamento (CE) 2006/2004 e messo a punto dalla Commissione europea per consentire alle autorità competenti in materia di tutela dei consumatori dei Paesi membri di collaborare nelle investigazioni che riguardano illeciti commessi in ambito transfrontaliero fornendo, allo stesso tempo, un *database* condiviso per lo scambio di informazioni su una piattaforma sicura.

9.9. "NUOVE FRONTIERE" DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: APPROFONDIMENTO SULL'UTILIZZO DELLE *APPLICATION* PER *SMARTPHONE* E *TABLET*

È stata avviata una complessa istruttoria in materia di *software* di vario tipo (giochi, musica, guide di natura diversa, *social network*, ecc.) che possono essere "scaricati" ed installati su *smartphone* e *tablet* per fornire a tali dispositivi alcune funzionalità aggiuntive (ad es., per la gestione del portfolio clienti o del calendario aziendale, per la condivisione di foto, video ed informazioni, per il monitoraggio dei propri movimenti bancari, per memorizzare ed elaborare testi o immagini, per localizzare ed essere localizzati da altri utenti, per redigere programmi in base alle proprie abitudini di consumo, per archiviare informazioni sulla salute).

L'Autorità ha richiesto informazioni ad alcuni produttori di sistemi operativi per *smartphone* e *tablet*, *leader* a livello mondiale nel settore.

Ne è emerso, anche esaminando alcune segnalazioni pervenute, che gli utenti che si avvalgono di tali applicazioni non sempre sono consapevoli dei rischi relativi al trattamento dei propri dati personali, soprattutto in ordine ai destinatari di tali dati, ai loro possibili utilizzi, al tempo di conservazione delle informazioni, alla loro archiviazione non sul dispositivo dell'utente, ma sulla *cloud* di un fornitore del servizio in modalità *web*, ecc.

L'Autorità sta esaminando i meccanismi volti ad informare gli utenti delle possibili modalità e finalità del trattamento dei dati personali e dei connessi rischi, quali *policy* interne, misure di sicurezza e ulteriori misure e attività di correzione ed *enforcement*, eventualmente previste per le ipotesi di violazione delle dette *policy* o di trattamenti illeciti dei dati personali.

Ciò, al fine di verificare la loro compatibilità con regole e princìpi *standard* in materia di protezione dei dati personali (quali i princìpi di proporzionalità e necessità), come emergenti anche da alcuni documenti elaborati dal Gruppo Art. 29 (cfr., *ex multis*: WP 163 del 12 giugno 2009 sui *social network online*; WP 171 del 22 giugno 2010 sulla pubblicità comportamentale).

10. PROPAGANDA ELETTORALE E ASSOCIAZIONI

L'Autorità si è occupata di una vicenda avente ad oggetto il trattamento di dati personali da parte di un'associazione a carattere notoriamente politico.

Con due distinte segnalazioni, era stata infatti contestata un'indebita divulgazione di dati personali sensibili relativi ad alcune aderenti, conseguente all'affissione nella bacheca (sita lungo il corso principale del paese) di un comunicato concernente l'espulsione delle segnalanti dall'associazione.

Questa aveva replicato che le istanti –la cui militanza politica era già nota presso la compagine locale, anche a seguito della loro partecipazione a precedenti appuntamenti elettorali– avevano appoggiato, nel corso di una pregressa campagna elettorale, una lista antagonista a quella ufficialmente sostenuta dal partito cui le stesse aderivano. L'affissione, pertanto, aveva risposto principalmente all'esigenza necessità di informare correttamente l'elettorato, disorientato dal comportamento delle segnalanti.

Al riguardo, il Garante ha ritenuto che l'affissione, considerato anche il contesto circoscritto e il momento in cui era avvenuta, risultava essere stata effettuata nel perseguimento di un legittimo interesse alla trasparenza e alla corretta informazione degli appartenenti alla compagine locale, sicché il correlato trattamento non poteva considerarsi illecito in relazione a tale profilo; essa costituiva inoltre una manifestazione del pensiero, prevista e disciplinata, sotto il profilo della protezione dei dati personali, dall'art. 136 ss. del Codice né, nel caso di specie, risultavano violati i limiti del diritto di cronaca avuto riguardo, in particolare, all'essenzialità dell'informazione.

Nondimeno, l'Autorità ha ritenuto sproporzionato il trattamento in relazione alla prolungata pubblicazione del comunicato (oggetto di affissione per alcuni mesi), essendo ormai venute meno, tenuto anche conto del ristretto contesto locale, le esigenze di trasparenza e chiarificazione prospettate dall'associazione. L'ulteriore diffusione è stata pertanto vietata (*Provv.* 23 dicembre 2010 [doc. *web* n. 1784951]).

Trattamento di dati sensibili da parte di un ente religioso

Sono pervenuti all'Autorità reclami e segnalazioni su possibili violazioni della disciplina in materia di protezione dei dati personali da parte di un ente religioso e di un'as-

sociazione di studi e ricerche nel campo della religiosità (di seguito "centro studi"), che in occasione dello svolgimento di una ricerca di tipo sociologico, avrebbero chiesto agli aderenti all'ente di compilare un questionario volto ad acquisire approfondite informazioni, anche di natura sensibile e, talora, riferite a terzi, su molteplici profili della loro vita personale (in specie, opinioni ed orientamenti politici; abitudini e tendenze sessuali; comportamenti in campo religioso; condizioni di salute; stili e scelte di vita su tematiche particolarmente delicate, quali l'interruzione della gravidanza).

A detta degli istanti il questionario, pur non contenendo i nominativi degli interessati, avrebbe comunque consentito di identificare i singoli compilatori, in virtù del possibile collegamento tra talune informazioni ivi contenute (quali l'anno di nascita, la città di residenza, la composizione del nucleo familiare, il ruolo rivestito nell'ambito dell'ente) ed altri dati sugli associati, detenuti dall'ente per altre finalità.

Le risultanze istruttorie non hanno consentito di ritenere provato l'avvenuto trattamento di dati personali di coloro che avevano aderito all'iniziativa (o di eventuali terzi), atteso che, stando alle dichiarazioni dell'ente e del centro studi, le informazioni fornite, per loro natura tali da non consentire l'identificazione "diretta" del compilatore o di terzi, non sarebbero state utilizzate, allo stato, dai soggetti coinvolti nell'attività di ricerca, neanche per l'identificazione "indiretta" degli interessati (cfr. art. 4, comma 1, lett. *b*) e *c*), del Codice); i soggetti contrari all'iniziativa, inoltre, non avevano compilato i questionari, sicché i loro dati personali non potevano essere stati trattati.

Tale ultima circostanza, confermata anche da ulteriori risultanze istruttorie, ha fatto venir meno ogni esigenza cautelare e, di conseguenza, ha reso non necessario l'esame delle richieste di blocco e di divieto del trattamento dei dati riferiti a taluni istanti.

Tuttavia, l'Autorità ha rilevato l'esistenza, presso l'ente, di un archivio nominativo e di altre fonti di informazione contenenti dati identificativi riferiti ai propri adepti, nonché di risorse tecnologiche presso il centro studi e la società esterna della quale il centro si era avvalso per l'analisi e l'elaborazione delle informazioni contenute nei questionari compilati, astrattamente in grado di permettere l'identificazione indiretta degli interessati, mediante un'interconnessione tra le informazioni riportate nei questionari –che, all'esito

dell'istruttoria curata dall'Autorità, erano ancora in possesso della menzionata società– e quelle conservate nel predetto archivio.

Analogamente, si è ritenuto che l'identificabilità indiretta degli interessati ai sensi del "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*" (Allegato A.4. al Codice) fosse agevolata, nel caso di specie, anche dal ristretto numero di membri dell'ente che avevano aderito all'iniziativa.

Pertanto, benché fossero stati adottati, in concreto, alcuni accorgimenti volti ad assicurare l'"anonimato" degli interessati, si è fatto presente che, soprattutto in considerazione della peculiare natura delle informazioni raccolte, tali accorgimenti avrebbero dovuto essere integrati con misure idonee ad impedire, fin dalla raccolta dei questionari compilati, anche l'indiretta identificabilità dei soggetti interessati alla rilevazione.

Il Garante ha pertanto prescritto al centro studi (in qualità di titolare della ricerca) di adottare accorgimenti idonei ad escludere il rischio di interconnessione tra i dati personali (in specie i nominativi) degli aderenti all'attività di ricerca (in possesso del solo ente religioso) e le informazioni contenute nei questionari, per evitare l'identificazione, sia pure in forma "indiretta", degli interessati.

A tal fine è stato prescritto di conservare i questionari in luoghi protetti da eventuali accessi indebiti, di non trasmetterli ad alcuno dei soggetti coinvolti nel progetto e di distruggerli al termine della ricerca. Al medesimo scopo, è stato disposto, nei confronti dell'ente, il divieto di comunicare agli altri soggetti coinvolti nel progetto di ricerca e per le finalità ad essa connesse, i dati personali riferiti ai propri adepti dei quali era in possesso, in qualità di autonomo titolare, per finalità di tipo associativo (art. 154, comma 1, lett. *d*), del Codice).

Infine, è stato prescritto al centro studi, in occasione di future iniziative di studio dalle quali possa discendere un'identificazione, sia pure in forma indiretta, dei soggetti coinvolti, di assicurare la scrupolosa osservanza e la concreta attuazione delle disposizioni contenute nel "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*", il cui rispetto costituisce condizione di liceità e correttezza del trattamento dei dati personali effettuato dai soggetti ai quali dette disposizioni si

riferiscono (artt. 12, comma 3 e 11, comma 1, lett. *a*), del Codice) (*Provv.* 1° aprile 2010 [doc. *web* n. 1721183]).

In un altro caso, un istituto che opera nel settore della ricerca sulla storia contemporanea aveva chiesto all'Autorità chiarimenti in ordine alla conformità al Codice della pubblicazione di taluni documenti, inerenti una rilevante vicenda storica (in specie, la sentenza di proscioglimento di uno degli imputati nel procedimento penale che ne è derivato, prima del dibattimento per estinzione del reato dovuta ad amnistia).

L'Autorità ha richiamato l'attenzione dell'istituto sulla necessità di conformare puntualmente il trattamento dei dati personali in esame sia all'art. 52, comma 7 e alle disposizioni contenute nella Parte II, Titolo VII, del Codice, sia alle prescrizioni contenute nel codice di deontologia e di buona condotta adottato in materia (*Provv.* 14 marzo 2001 [doc. *web* n. 1556419]), con particolare riferimento a quanto disposto dal Capo III contenente "*regole di condotta per gli utenti e condizioni per la liceità dei relativi trattamenti*".

Tenuto conto della peculiare natura dei dati oggetto di trattamento, si è fatto altresì presente che lo stesso era stato già autorizzato dal Garante nei termini previsti dal capo V dell'autorizzazione n. 7 del 16 dicembre 2009, relativa al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici (*Nota* 12 gennaio 2010).

11. Le attività economiche e i rapporti di lavoro

11.1. Settore bancario

Nel periodo di riferimento l'attività in questo settore è stata principalmente rivolta alla trattazione dei casi prospettati a diverso titolo all'Autorità.

In uno di essi, in particolare, un reclamante aveva fatto presente che la moglie, dovendo svolgere normali operazioni *online* su un conto corrente cointestato con lo stesso reclamante, aveva utilizzato le credenziali a suo tempo attribuitele dalla banca per accedere ai servizi in rete. Benché le credenziali fossero pertinenti al solo conto cointestato, la digitazione aveva consentito di accedere ad un altro conto corrente di cui soltanto il reclamante era titolare ed intestatario, sicché il coniuge aveva avuto la possibilità di conoscere le movimentazioni bancarie su di esso effettuate ed il relativo saldo. Di conseguenza l'interessato aveva chiesto al Garante, previa adozione di un *provvedimento* di blocco dei dati trattati, di prescrivere alla banca le misure necessarie per rendere il suddetto trattamento conforme a legge.

Le risultanze istruttorie hanno consentito di accertare una indebita comunicazione a terzi (nel caso di specie, al coniuge del reclamante) di dati bancari, per omessa osservanza, da parte degli incaricati della banca, delle istruzioni loro impartite.

Pertanto, pur avendo verificato che la banca aveva adottato le misure "minime" di sicurezza a protezione dei dati dei clienti (artt. 33 e 34 del Codice; regole 1-26 dell'Allegato B.), il Garante ha prescritto di rafforzare le misure di sicurezza "idonee" di cui all'art. 31 del Codice, in modo da garantire la scrupolosa vigilanza sull'operato degli incaricati, sensibilizzarli al rispetto delle istruzioni ricevute in occasione di specifiche iniziative di formazione del personale e ridurre al minimo il rischio di errori operativi (*Provv.* 11 febbraio 2010 [doc. *web* n.1705119]).

In un altro caso, il reclamante aveva rappresentato che il proprio coniuge, nell'atto introduttivo del procedimento di separazione personale, aveva fatto riferimento ad informazioni che lo riguardavano, relative a rapporti contrattuali con la banca, producendo anche specifici documenti bancari. L'interessato si era quindi rivolto al Garante affinché fosse accertata l'illiceità della comunicazione a terzi dei suoi dati personali.

Dalle risultanze istruttorie è emerso che presso la banca era stato effettuato, in assenza di legittimo presupposto, un accesso ai dati bancari riferiti al reclamante. Ciò verosimilmente per il comportamento dell'incaricato della banca, che, senza fornire giustificazione, aveva consultato la posizione del reclamante, in un orario in cui l'interessato, unico soggetto deputato a ricevere tali informazioni, risultava inequivocabilmente in servizio presso la propria sede di lavoro (cfr. artt. 4, comma 1, lett. *h*), 30, 167 del Codice).

Anche in questo caso, il Garante, ha prescritto di rafforzare le misure di sicurezza "idonee" di cui all'art. 31 del Codice (*Provv.* 18 marzo 2010 [doc. *web* n. 1715015]).

In un ulteriore caso, l'interessato aveva segnalato che un importante gruppo bancario aveva contattato telefonicamente sua moglie, titolare di un mutuo chirografario appoggiato per il versamento delle rate su un conto corrente intestato in via esclusiva allo stesso segnalante ed acceso presso una banca del gruppo, per sollecitare il pagamento di una mensilità ancora non corrisposta. In tale occasione, tuttavia, la dipendente preposta avrebbe reso noto al coniuge dell'interessato anche ulteriori vicende concernenti lo stato del conto corrente (cioè l'esistenza di un fido concesso al titolare del rapporto e l'avvenuto sconfinamento rispetto al fido). Ritenendo tale comportamento contrario alla disciplina di protezione dei dati personali, l'interessato aveva chiesto al Garante l'adozione di misure atte ad impedire il ripetersi di episodi analoghi.

Al riguardo, in base ai princìpi in materia di trattamento di dati personali nell'esercizio dell'attività di recupero crediti (v. *Provv.* 30 novembre 2005 [doc. *web* n. 1213644]), il Garante ha ritenuto pertinente e non eccedente rispetto alla finalità di recupero crediti la comunicazione al mutuatario del numero di conto corrente, del nominativo del relativo intestatario, della banca di appoggio e dell'esito negativo del tentativo di addebito del conto per incapienza del medesimo, sempre che al titolare del rapporto di conto corrente fosse stata resa un'adeguata informativa. Ha, però, considerato sproporzionato il trattamento di informazioni concernenti l'esistenza di "fidi" o eventuali loro "sconfinamenti" del tutto ininfluenti ai fini di una corretta informazione del mutuatario sulle vicende strettamente inerenti al saldo dei ratei in scadenza. Nel caso in questione, tuttavia, le risultanze istruttorie non hanno consentito di ritenere comprovata la lamentata comunicazione anche di informazioni strettamente riguardanti il conto corrente del segnalante.

Dal momento che le misure "minime" di sicurezza poste a presidio dei dati trattati nell'esercizio delle attività di recupero crediti (artt. 33-35 del Codice e Allegato B. al Codice) erano state adottate, il Garante ha prescritto alla banca e alla società finanziaria di richiamare il responsabile e gli incaricati del trattamento al rispetto delle istruzioni già impartite.

L'Autorità ha altresì prescritto alla società finanziaria di comunicare al mutuatario solo i dati bancari pertinenti rispetto alle finalità di informare il titolare del finanziamento sulle vicende relative al mutuo e di consentirgli di regolarizzare la posizione debitoria; inoltre, al fine di verificare la tipologia e la pertinenza delle informazioni rese al debitore in caso di contestazioni, ha suggerito di privilegiare l'invio dei solleciti di pagamento mediante l'impiego di idonee modalità, quali, per esempio, la comunicazione elettronica all'indirizzo e-mail fornito dal debitore o, in difetto, la spedizione in plico chiuso presso il suo domicilio (*Provv.* 21 ottobre 2010 [doc. *web* n. 1771017]).

Un comune aveva lamentato la comunicazione da parte di una banca agli studi legali che assistevano alcuni creditori in procedimenti esecutivi presso terzi (nel caso di specie, la banca stessa) promossi nei confronti del Comune, gli estremi identificativi ed il nominativo delle parti di altri procedimenti esecutivi promossi nei confronti del comune medesimo. Ciò mediante l'invio di una sola missiva all'indirizzo di tutti i creditori procedenti.

Tale comunicazione, originata da procedimenti pendenti avanti al giudice civile, era eccedente ai sensi dell'art. 11, comma 1, lett. *d*), del Codice, rispetto alla finalità perseguita (consistente nell'informare i creditori procedenti circa le modalità con le quali la banca, in qualità di terzo, aveva provveduto ad adempiere agli obblighi imposti al custode dall'art. 547 c.p.c.), anche in considerazione del fatto che ciascun destinatario della comunicazione, ancorché creditore procedente in un distinto procedimento esecutivo, era terzo rispetto agli altri procedimenti. Poiché il comune non aveva prestato il consenso alla comunicazione (art. 23 del Codice) né ricorrevano i presupposti alternativi di cui all'art. 24 del Codice, la comunicazione stessa è stata ritenuta in violazione degli artt. 11, comma 1, lett. *d*) e 23 del Codice. Il Garante ha riservato ad un autonomo procedimento le valutazioni relative all'eventuale applicazione di sanzioni amministrative.

11.2. TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLA CENTRALE DEI RISCHI GESTITA DALLA BANCA D'ITALIA E DEI SISTEMI DI INFORMAZIONE CREDITIZIA (SIC)

Anche nel corso del 2010 sono pervenute all'Autorità segnalazioni e reclami riguardanti il trattamento dei dati personali posto in essere da banche dati pubbliche e private (Sistemi di informazione creditizia-SIC e Centrale dei rischi gestita dalla Banca d'Italia) e dalle banche e finanziarie che agiscono in qualità di partecipanti a tali sistemi.

Le segnalazioni hanno riguardato soprattutto l'informativa da fornire agli interessati, nonché il rispetto delle norme di condotta previste dal "*Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*" (*Provv.* 16 novembre 2004 [doc. *web* n. 1556693] Allegato A.5. al Codice), che costituiscono condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali effettuati dai gestori e dagli utenti dei sistemi di informazioni creditizie (SIC).

Al riguardo, il Garante ha ribadito che i dati conservati nei SIC devono essere sempre corretti ed aggiornati e che l'iscrizione di una posizione debitoria in tali banche dati è lecita solo se ne è stato dato preavviso all'interessato.

Più in dettaglio, in un caso l'interessato aveva segnalato di essere venuto a conoscenza, in occasione di una richiesta di mutuo, dell'esistenza di una segnalazione negativa a suo nome presso un SIC, effettuata da parte di una finanziaria dalla quale aveva in passato ricevuto un prestito. Le risultanze istruttorie hanno consentito di accertare che il segnalante aveva pagato tutte le rate previste, ma che, presumibilmente per errore, una di tali rate non era stata registrata dalla società finanziaria. Quest'ultima, inoltre, prima di procedere all'iscrizione del nominativo dell'interessato nel SIC, non aveva provveduto ad inviargli l'avviso dell'imminente registrazione del suo nominativo nei SIC, come previsto dall'art. 4, comma 7, del suddetto codice di deontologia e di buona condotta. In considerazione di quanto sopra esposto, il Garante ha prescritto alla società finanziaria di disporre la cancellazione dal SIC dei dati riferiti al finanziamento sottoscritto dall'interessato (*Provv.* 16 settembre 2010 [doc. *web* n. 1753816]).

In un'altra segnalazione, relativa ad una complessa vicenda, una società ha rappresentato

di avere riscontrato la presenza del proprio nominativo in un sistema di informazioni creditizie, quale richiedente un prestito finalizzato. La segnalazione al SIC era stata effettuata da una finanziaria, alla quale la segnalante asseriva di non aver chiesto alcun finanziamento. Nel riscontro fornito all'Autorità, la società finanziaria rappresentava di aver ricevuto i dati da un'altra società, per valutare la richiesta di concessione di un fido per l'acquisto di beni formulata dalla segnalante a quest'ultima società. La comunicazione di dati e l'avvio dell'istruttoria nella richiesta di finanziamento erano, tuttavia, avvenute senza la previa informativa richiesta dall'art. 13 del Codice.

Il trattamento è risultato, pertanto, in contrasto con la previsione dell'art. 13 del Codice e non conforme alle regole di comportamento previste dal citato codice di deontologia.

Il Garante ha pertanto prescritto alle società titolari del trattamento rispettivamente di formulare un'informativa in stretta aderenza a quanto previsto dall'art. 13 del Codice e di osservare scrupolosamente e dare concreta attuazione alle regole di comportamento stabilite dal codice di settore (*Provv.* 6 maggio 2010 [doc. *web* n. 1737818]).

In un altro caso un segnalante, al quale era stato rifiutato un finanziamento, aveva appreso che presso un SIC risultava, a suo nome, un'operazione di "prestito rinunciato", a suo dire non corrispondente al vero.

Dall'istruttoria è emerso che tale dato non era esatto, non era stata fornita all'interessato l'informativa, ed il riscontro alle richieste avanzate dall'interessato stesso ai sensi dell'art. 7 del Codice era stato tardivo.

Pertanto il Garante ha prescritto alla banca di garantire il rispetto delle regole di comportamento stabilite dal codice di settore e di sensibilizzare in tal senso gli incaricati del trattamento, ribadendo l'essenzialità del rispetto di tale regole, nonché di assicurare che sia fornito un idoneo e tempestivo riscontro nei termini di legge a tutte le istanze ritualmente proposte ai sensi dell'art. 7 del Codice (*Provv.* 11 marzo 2010 [doc. *web* n. 1715024]).

L'Autorità ha poi dato corso a una segnalazione inviata dal presidente del consiglio di amministrazione di due società, il quale ha rappresentato di essere venuto a conoscenza della presenza di segnalazioni a carico delle società stesse presso il *cd.* "*servizio di prima informazione*" presso la Centrale dei rischi della Banca d'Italia, riguardanti richieste di