sicurezza, nel rispetto del segreto professionale (punto 3.2. delle citate linee-guida del 14 giugno 2007; artt. 25, comma 1, lett. *c*), *d*) ed *e*), 39, comma 4, 41, comma 8 e 42 d.lgs. 9 aprile 2008, n. 81; v. anche il parere del Garante del 31 marzo 2008 [doc. *web* n. 1504941]). Nel caso di specie il medico competente avrebbe dovuto salvaguardare la segretezza e la sicurezza delle informazioni contenute nella documentazione sanitaria in suo possesso, trasmettendone copia in busta chiusa al datore di lavoro in modo tale da consentire a quest'ultimo di consegnarla all'interessato che ne aveva fatto richiesta. A seguito dell'intervento del Garante, l'azienda ospedaliera ha chiarito di aver accertato che la copia della cartella sanitaria e di rischio da consegnare al dipendente non necessita di autenticazione ed ha fornito idonee assicurazioni in relazione al rispetto, per il futuro, della disciplina sulla protezione dei dati personali (nota 23 dicembre 2011).

Dati sanitari del personale militare

Si richiama qui, perché attiene al trattamento dei dati di dipendenti, anche il parere reso al Ministero della difesa (parere 16 febbraio 2011 [doc. *web* n. 1797055]) sullo schema di decreto concernente le modalità di caricamento dei dati sanitari di emergenza nella tessera personale di riconoscimento del personale militare, Carta multiservizi della difesa (CMD), il cui testo tiene conto degli approfondimenti e delle indicazioni rese dall'Ufficio del Garante nel corso di riunioni e contatti informali, avviati sin dal 2008 (cfr. Relazione 2008, p. 142; v. anche par. 1.2.3.).

Nel corso del 2010, su sollecitazione dello stesso Ministero erano stati avviati, inoltre, approfondimenti sulla prassi di comunicare all'autorità di pubblica sicurezza i nominativi dei militari affetti da patologie psico-neurologiche ai fini della revoca dell'autorizzazione di Polizia a detenere armi a titolo privato (v. Relazione 2010, p. 140) nonché con riferimento all'indicazione della diagnosi nei certificati medici attestanti lo stato di malattia dei militari. A seguito di tali approfondimenti e delle indicazioni rese dall'Ufficio del Garante ai competenti uffici del Ministero, alcune proposte di modifica della normativa –in particolare per quanto attiene all'indicazione della diagnosi nei certificati medici e all'introduzione del sistema del cd. "doppio certificato"– sono state sottoposte nel 2011 all'Autorità, che ha espresso parere ai sensi dell'art. 154, comma 4, del Codice (provv. 22 settembre 2011 [doc. *web* n. 1844183] v. par. 1.2.3.)

10.6. PREVIDENZA

Un ufficio periferico dell'Istituto nazionale della previdenza sociale ha investito l'Autorità, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, di una richiesta finalizzata alla comunicazione ad un'azienda ospedaliera universitaria di dati concernenti la sussistenza di eventuali posizioni previdenziali nel casellario dei lavoratori attivi relativi ad un gruppo di lavoratori identificato in un arco temporale predeterminato. Finalità della comunicazione richiesta era quella dell'azienda di procedere a verifiche a campione sui propri dipendenti correlate al divieto dello svolgimento di attività incompatibili con il rapporto di pubblico impiego, come previsto dagli artt. 60-64, d.P.R. n. 3/1957, dall'art. 53, d.lgs. n. 165/2001 e dall'art. 1, commi da 56 a 65, l. n. 662/1996.

Il Garante, impregiudicato l'esercizio da parte dell'azienda delle prerogative riconosciute dall'art. 22, l. n. 241/1990, non ha accolto l'istanza presentata, sia per l'assenza di un'espressa previsione normativa che in via diretta ammettesse detta comunicazione, sia per la presenza di una puntuale disciplina (art. 39, comma 28, l. n. 27 dicembre 1997, n. 449 "Misure per la stabilizzazione della finanza pubblica") che consente di acquisire i dati necessari all'accertamento di eventuali situazioni di incompatibilità mediante la Guardia di finanza (provv. 24 novembre 2011 [doc. *web* n. 1880524]).

Nel corso dell'anno l'Ufficio ha ricevuto alcune segnalazioni con le quali si lamentava che una direzione dell'Inps aveva inviato comunicazioni contenenti verbali di accertamento dell'invalidità civile a persone diverse dagli interessati. Facendo seguito alla richiesta di informazioni ed alle indicazioni del Garante, l'Inps ha chiarito che si era trattato di un errore materiale ed ha assicurato di aver richiamato il personale addetto al rispetto delle regole sul trattamento dei dati personali (nota 20 gennaio 2012).

11. LE ATTIVITÀ ECONOMICHE

11.1. SETTORE BANCARIO

Provvedimento in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

Si è conclusa nel 2010 l'attività ispettiva avviata dal Garante presso alcuni importanti istituti e gruppi bancari, sulla base di numerose segnalazioni, che lamentavano indebiti accessi da parte di dipendenti alle informazioni bancarie dei clienti.

A seguito di tale attività il Garante ha adottato specifici provvedimenti (v. Relazione 2009, pp. 152-154, e Relazione 2010, pp. 132-134) ed ha altresì individuato profili problematici di carattere generale sul cui approfondimento ha coinvolto l'Abi. Quest'ultima ha elaborato un documento, in forma aggregata e anonima, relativo ad una rilevazione cui hanno partecipato "340 tra banche e gruppi bancari, che fanno complessivamente riferimento a 441 banche operanti sul territorio italiano" e che ha permesso una più dettagliata conoscenza dei meccanismi del settore, per una migliore definizione dell'intervento dell'Autorità.

In questo quadro, in assenza di una normativa che obblighi le banche a tracciare tutte le operazioni, l'Autorità ha adottato in data 12 maggio 2011 un provvedimento "in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie", pubblicato in G.U. 3 giugno 2011, n. 127 [doc. *web* n. 1813953], nel quale è stata prescritta agli istituti bancari l'adozione di rigorose misure.

In particolare è stato disposto che ogni operazione di accesso ai dati dei clienti (che comporti movimentazione di denaro o sia di semplice consultazione), effettuata da qualunque figura all'interno della banca, dovrà essere tracciata e registrata in un apposito log, nel quale devono essere contenuti: il codice identificativo del dipendente; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; il codice del cliente ed il tipo di rapporto contrattuale "consultato" (numero del conto corrente, fido, mutuo, deposito titoli). Tale misura ha lo scopo di assicurare che la banca sappia sempre il soggetto che ha avuto accesso ad un determinato conto corrente o ha effettuato operazioni ed il momento in cui ciò è avvenuto. I file di log di tracciamento delle operazioni, comprese quelle di semplice consultazione, dovranno essere conservati per almeno 24 mesi. Le banche, inoltre, dovranno prevedere l'attivazione di *alert* che individuino comportamenti anomali o a rischio (es. consultazioni massive, accessi ripetuti su uno stesso nominativo).

Almeno una volta l'anno la gestione dei dati bancari dovrà essere oggetto di un'attività di controllo interno, per verificare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalla normativa vigente. Il controllo, adeguatamente documentato, dovrà essere eseguito da personale diverso da quello che ha accesso ai dati dei clienti. Inoltre, verifiche sulla legittimità e liceità degli accessi, sull'integrità dei dati e delle procedure informatiche dovranno essere effettuate anche a posteriori, sia a campione sia a seguito di segnalazione.

Alle banche è stato infine raccomandato, come misura opportuna, di comunicare al cliente eventuali accessi non autorizzati al proprio conto e di rendere note al Garante eventuali violazioni di particolare rilevanza (per quantità, qualità dei dati, numero dei clienti).

11.2. INFORMAZIONI COMMERCIALI

Parziale modifica del provvedimento Ancic sull'esonero dell'informativa

Con provvedimento del 15 dicembre 2011 [doc. *web* n. 1862497] su istanza dell'Ancic (Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito) sono state rese meno onerose per le società associate, le modalità per rendere l'informativa semplificata agli interessati, in occasione del trattamento dei loro dati per finalità di informazione commerciale, già stabilite nel provv. 14 maggio 2009 [doc. *web* n. 1616828] (cfr. Relazione 2009, pp. 158-159).

In particolare, è stata prevista la pubblicazione, nella versione cartacea di "Pagine Gialle Lavoro", di un testo di informativa identico a quella attualmente resa, inserendo invece, alla voce "Ancic" riportata nell'elenco alfabetico di "Pagine Bianche" un semplice rimando al testo pubblicato su "Pagine Gialle Lavoro".

Il Garante ha previsto altresì l'inserimento, sui siti *web* di "Pagine Gialle" e di "Pagine Bianche", di appositi *banner* che consentano l'immediata apertura del testo dell'informativa e la pubblicazione, in maniera permanente sul proprio sito *web*, da parte di ciascuna società di informazione commerciale aderente ad Ancic, dell'informativa prevista dall'art. 13 del Codice, da evidenziarsi adeguatamente in autonomi riquadri di immediata consultazione.

L'Autorità, infine, ha prescritto, quale misura opportuna, che Ancic continui a tenere costantemente aggiornato l'elenco delle società di informazione commerciale aderenti, allo stato già presente sul sito *web* dell'Associazione.

11.3. ALTRE ATTIVITÀ IMPRENDITORIALI

Rientra in questo settore una eterogenea casistica di seguito esposta in sintesi.

Nell'ambito del trattamento dei dati personali degli utenti e dei lavoratori di *call center*, l'Autorità si è attivata a seguito di una segnalazione, che aveva rappresentato possibili profili di violazione della disciplina di protezione dei dati in relazione a un sistema di registrazione delle telefonate "in entrata" che una società stava implementando presso i propri gestori del servizio di *customer satisfaction*. Il sistema, diretto a migliorare la qualità del servizio di assistenza alla clientela attraverso un'analisi delle attività di "gestione" dell'utente da parte degli stessi *call center* (anche in vista di un eventuale miglioramento dei processi formativi del relativo personale), avrebbe garantito il rispetto dei princìpi del Codice attraverso opportuni accorgimenti volti, in particolare, a circoscrivere il trattamento dei dati personali degli interessati (campionatura delle telefonate registrate; alterazione della voce degli interlocutori; eliminazione degli orari di registrazione e dei primi secondi di conversazione; ecc.). L'impiego del sistema sarebbe stato preceduto da un'apposita informativa ai lavoratori interessati, mentre alla clientela tale informativa sarebbe stata resa in forma semplificata in occasione del collegamento con l'operatore, con possibilità di ricevere un'informativa più dettagliata collegandosi al sito della società.

All'esito dell'istruttoria condotta, il Garante, pur riconoscendo come meritevoli le finalità perseguite dalla società, ha tuttavia rilevato che l'informativa predisposta per l'utenza in occasione del contatto telefonico non dava sufficientemente conto delle finalità del trattamento, né indicava come poter accedere ad un'informativa più dettagliata. L'Autorità ha quindi prescritto alla società di integrare in tal senso l'informativa sintetica.

Il Garante ha poi ricordato come il trattamento in esame potesse essere effettuato dalla società solo con il consenso espresso degli interessati o in presenza di uno dei presupposti alternativi previsti dall'art. 24 del Codice. Considerato che un eventuale diniego del consenso avrebbe vanificato le finalità migliorative perseguite dalla Società, il Garante è intervenuto con un provvedimento di bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice), ritenendo che in questo caso il legittimo interesse del titolare del trattamento in riferimento a proprie esigenze di natura organizzativa e produttiva non potesse essere

considerato minusvalente rispetto ai diritti e alle libertà fondamentali degli interessati (provv. 9 febbraio 2011 [doc. *web* n. 1797032], v. al riguardo anche il par. 10.1.4.).

In un altro caso, l'Autorità è stata chiamata a pronunciarsi a seguito della richiesta di esonero di informativa da parte di una società operante nel settore dell'energia per l'allestimento di un sistema informativo volto a fornire ai vertici aziendali un costante aggiornamento sulla normativa in materia di energia e ambiente, nonché indicazioni sui soggetti istituzionali impegnati nel settore, compresi gli *opinion leader* regionali esperti in materia. In particolare, la società aveva chiesto di essere esonerata dall'obbligo di rendere l'informativa, sia in relazione al trattamento dei dati personali presenti nei siti *web* di tredici regioni italiane, concernenti soltanto il ruolo professionale dei predetti soggetti istituzionali, sia riguardo alle informazioni contenute nelle "relazioni" redatte all'esito di eventuali interlocuzioni con essi intervenute, ai sensi dell'art. 13, comma 5, del Codice.

L'Autorità, con provvedimento del 31 marzo 2011 [doc. *web* n. 1810147] non ha formulato alcun rilievo sulla realizzazione della banca dati normativa interna, non potendosi configurare rispetto ad essa alcun trattamento di dati personali.

Il Garante ha poi valutato che gli obiettivi del progetto, a sostegno di specifici uffici interni di gestione delle relazioni istituzionali, non fossero, in via generale, incompatibili con la finalità di informazione e trasparenza sottesa alla divulgazione via internet dei dati da parte degli enti pubblici titolari dei siti *web*. Inoltre, ha ritenuto di escludere i dati contenuti nelle "relazioni" relative agli incontri con "i soggetti decisori", dall'applicazione dell'art. 13, commi 4 e 5, del Codice, trattandosi di informazioni acquisite direttamente presso gli interessati nell'ambito dell'ordinaria attività lavorativa, peraltro oggetto di limitata divulgazione all'interno della società (soltanto 12 posizioni) nel rispetto degli ordinari vincoli gerarchici.

Pertanto, l'Autorità, ravvisando una manifesta sproporzione tra i mezzi necessari per rendere l'informativa e il diritto tutelato (stante la vastità del numero dei soggetti che istituzionalmente si occupano –anche solo a livello regionale– di energia ed ambiente), ha esonerato dall'obbligo di rendere l'informativa individuale agli interessati, in relazione al trattamento dei soli dati concernenti gli attori istituzionali acquisiti dai suindicati siti *web*, prescrivendo alla società di porre in evidenza, nella sezione *"compliance"* del proprio sito *web*, le caratteristiche del sistema

informativo e di specificare le finalità del trattamento, i tipi di dati che verranno reperiti negli specifici siti *web* regionali e le categorie di soggetti che formeranno oggetto di ricognizione.

In relazione ad un'ipotesi di fusione per incorporazione, l'Autorità si è espressa in merito all'istanza di una primaria società editoriale, che ha chiesto, in via principale, di essere esonerata dall'obbligo di rendere l'informativa agli interessati (tra cui, in particolare, gli abbonati e gli utenti dei siti internet) ed in via subordinata, –considerato che i trattamenti di dati riguardavano la stessa società ed alcune società da essa interamente controllate– di poter rendere la predetta informativa con modalità semplificate. L'istanza era motivata dal fatto che l'informativa secondo le modalità ordinarie avrebbe comportato, per il numero elevatissimo di interessati (oltre dieci milioni di persone) l'impiego di mezzi manifestamente sproporzionati rispetto ai diritti tutelati.

Con riferimento a richieste simili, ovvero di esonero dall'obbligo di rendere l'informativa in casi di fusione per incorporazione in ambito bancario (cfr. provv.ti 11 dicembre 2008 [doc. *web* n. 1584328]; 19 dicembre 2008 [doc. *web* n. 1584272]; 8 aprile 2009 [doc. *web* n. 1609999]), il Garante aveva rilevato, come affermato anche in giurisprudenza (Cass. civ. S.u., 8 febbraio 2006, n. 2637), che *"per effetto della fusione per incorporazione la società incorporante assume i diritti e gli obblighi della società incorporata, proseguendo, in tutti i rapporti (attivi e passivi) della medesima (anche processuali) anteriori alla fusione (art. 2504-bis, comma 1, c.c.)"*, e che pertanto anche i dati personali relativi a detti rapporti sono destinati ad essere trattati senza soluzione di continuità dalla società incorporante, la quale diviene unico titolare del trattamento senza dover procedere ad una (nuova) raccolta di dati.

Analogamente, nel caso in esame, si è osservato che la società incorporante avrebbe continuato l'attività delle società incorporate, nonché "il trattamento dei dati precedentemente svolto dalle incorporate (...), secondo le stesse modalità e per le medesime finalità di cui alle informative fornite dalle società precedenti titolari".

Pertanto, con provvedimento del 1° dicembre 2011 [doc. *web* n. 1872641], in attuazione dei princìpi di "correttezza" (art. 11, comma 1, lett. *a*), del Codice), "semplificazione, armonizzazione ed efficacia" (art. 2, comma 2, del Codice), l'Autorità ha prescritto alle società coinvolte nella predetta operazione di fornire agli interessati (attraverso i propri siti

web) i necessari aggiornamenti rispetto all'informativa resa dalle società oggetto della fusione e, tra essi, in particolare, di esplicitare la nuova denominazione del titolare del trattamento e gli estremi identificativi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali.

Trattamento dati personali dei disabili per l'acquisto di un'autovettura

Su sollecitazione della Federazione italiana dei concessionari di auto (Federauto) l'Autorità, con il provvedimento del 16 febbraio 2011 [doc. *web* n. 1792975], si è pronunciata sul trattamento di dati personali effettuato in occasione dell'acquisto di veicoli per i soggetti disabili, in vista dell'eventuale concessione dei benefici fiscali di legge, stabilendo le modalità di attuazione dei princìpi di necessità, pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *d*), del Codice).

A tal fine, il Garante ha previsto che gli organi competenti ad accertare le patologie per le quali viene previsto il beneficio fiscale indichino nelle certificazioni i soli dati pertinenti, completi e non eccedenti rispetto alle finalità per le quali debbono essere successivamente trattati nel procedimento di valutazione, e che gli operatori economici del settore trattino soltanto i dati effettivamente necessari per la definizione della specifica procedura valutativa; in particolare le imprese devono raccogliere la sola documentazione richiesta dalla legge.

Il Garante ha poi prescritto che i concessionari rendano agli interessati un'informativa dettagliata, indicando espressamente che i dati personali forniti –anche sensibili– potranno essere comunicati ad officine autorizzate in vista degli eventuali adattamenti da apportare ai veicoli acquistati, provvedendo, in quest'ultimo caso, ad acquisire anche il relativo consenso.

È stato inoltre previsto che trascorsi dieci anni, i dati personali, compresi quelli sanitari, salvo altre esigenze di conservazione (ad es. per controversie giudiziarie pendenti), dovranno essere distrutti, cancellati o trasformati in forma anonima. Infine, considerata l'ampiezza e la delicatezza delle informazioni trattate, l'Autorità ha raccomandato ai concessionari, alle imprese e alle officine autorizzate di adottare adeguate misure di sicurezza.

11.4. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Nel corso dell'anno, il Garante si è pronunciato in relazione ad una serie di istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società del settore privato.

Un'azienda che produce componenti meccanici di elevata precisione (in particolare, sfere di acciaio aventi caratteristiche qualitative e geometriche valutabili nell'ordine di centesimi di micron), destinati ad essere impiegati in diversi settori industriali, aveva chiesto di poter conservare per ventiquattro mesi le immagini acquisite attraverso il sistema di videosorveglianza in uso.

Avendo subìto numerosi atti di sabotaggio da parte di ignoti dopo la conclusione delle normali fasi di ispezione e di collaudo del "prodotto finito", la società, dal 2003, previo accordo con le rappresentanze sindacali unitarie, si era dotata del sistema per preservare la produzione e la competitività aziendale, evitando, al contempo, danni d'immagine che si sarebbero potuti riverberare anche sui livelli occupazionali.

L'Autorità ha rilevato che i ripetuti atti illeciti subiti dalla società in numerosi casi erano stati accertati soltanto a distanza di notevole tempo dalla loro commissione, al termine di fisiologici periodi di stoccaggio delle componenti meccaniche o, addirittura, dopo la loro successiva commercializzazione.

Pertanto, il Garante, ritenendo che l'installazione del sistema di videosorveglianza e l'allungamento dei tempi di conservazione delle immagini trovassero giustificazione in esigenze di tutela del patrimonio aziendale e di prevenzione di possibili atti di sabotaggio forieri di notevoli danni per l'azienda (oltre che per l'incolumità dei fruitori dei sistemi prodotti), ha accolto la richiesta di allungamento dei tempi di conservazione delle immagini in quanto conforme ai princìpi di non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*), del Codice (provv. 7 luglio 2011 [doc. *web* n. 1836347]).

Sempre in sede di verifica preliminare l'Autorità ha accolto la richiesta di allungare a 90 giorni i tempi di conservazione delle immagini registrate dal sistema di videosorveglianza di una società produttrice di fotomaschere, strumenti fondamentali per la realizzazione di dispositivi elettronici a circuito integrato (componentistica elettronica, *chips*, *smart card*, ecc.).

La richiesta di autorizzazione era stata motivata con l'esigenza sia di migliorare il livello di tutela della proprietà aziendale, sia di acquisire la qualità di "fornitore" di una società committente straniera, "leader mondiale" nel settore della sicurezza e fornitore ufficiale di molti governi, soggetta agli specifici protocolli di sicurezza fissati dagli *standard* ISO15408

(*"Common Criteria"*) e ISO17799 (codice di buona pratica per la gestione della sicurezza dell'informazione), di cui essa richiedeva l'osservanza anche ai propri fornitori.

L'Autorità ha autorizzato la conservazione limitatamente alle immagini degli eventi relativi agli effettivi allarmi, tenendo conto non solo dell'ubicazione isolata del sito e del delicato settore produttivo in cui opera l'azienda, ma anche della specifica attenzione, posta anche a livello internazionale, all'osservanza di elevati *standard* di sicurezza nelle produzioni relative al settore elettronico ed informatico.

In proposito, l'Autorità ha ritenuto che alcuni specifici *standard* ISO (definiti dalla *International Organization for Standardization*, di cui è membro anche l'Ente nazionale italiano di unificazione-Uni), recanti "specificazioni tecniche" volte a garantire rigorosi livelli di sicurezza, seppur giuridicamente non vincolanti, comunque fissano stringenti parametri qualitativi in settori di rilevante interesse pubblico e, al contempo, tecnologicamente assai complessi. In tal senso si è rilevato che spesso sono le stesse autorità pubbliche a promuoverne l'osservanza o fare diretto riferimento ad essi in atti ufficiali, mentre in ambito privatistico, stante l'esistenza di una consolidata prassi al loro inserimento negli schemi contrattuali nazionali ed esteri, tali norme sono divenute un punto di riferimento ineludibile in occasione della fornitura di opere o della prestazione di servizi ad alto contenuto tecnologico (provv. 14 luglio 2011 [doc. *web* n. 1836335]).

L'Autorità ha poi esaminato l'istanza di una primaria società di spedizione di documenti e pacchi in tutto il mondo, in prevalenza per via aerea, di prolungare fino a 30 giorni i tempi di conservazione delle immagini registrate presso i magazzini situati in alcuni aeroporti italiani.

La richiesta è stata giustificata con l'esigenza sia di rafforzare la sicurezza del patrimonio aziendale e delle spedizioni, sia di mantenere uno *standard* di sicurezza elevato, richiesto dalle regole del sistema di certificazione volontaria sulla qualità e sicurezza dei servizi aerei gestito da *"Transported Asset Protection Association"* (*TAPA*), ritenuto un "parametro di riferimento per gli adempimenti finalizzati a garantire la sicurezza dei trasporti e delle merci".

L'Autorità, nel rilevare che la società è soggetta a stringenti norme poste da regolamenti comunitari e, in via amministrativa, dall'Ente nazionale per l'aviazione civile (Enac), ha autorizzato la conservazione delle immagini al solo fine di consentire l'accertamento, da parte

dell'autorità giudiziaria, di eventuali illeciti verificatisi in occasione delle spedizioni, considerando che essi sono solitamente rilevabili solo dopo l'arrivo a destinazione della merce, spesso trattenuta per vari giorni nei magazzini.

Circa le norme poste dalla *"Transported Asset Protection Association"* (*TAPA*), è stato ritenuto che esse, pur essendo giuridicamente non vincolanti, sono comunemente considerate nel settore come fondamentali per garantire al meglio la sicurezza delle merci trasportate e, conseguentemente, per ridurre le perdite sofferte dalla catena di approvvigionamento internazionale, prevenendo furti e danneggiamenti, legati, in alcuni casi, anche ad atti di terrorismo internazionale (provv. 10 novembre 2011 [doc. *web* n. 1877751]).

L'Autorità si è da ultimo pronunciata in merito all'istanza di una società concessionaria dell'Anas di poter conservare per venti giorni alcune immagini acquisite (con l'accordo delle rappresentanze sindacali) attraverso il sistema di videosorveglianza in uso presso le stazioni autostradali del tratto in concessione.

L'Autorità ha ritenuto tale periodo di conservazione giustificato in ragione sia della programmazione dei prelievi presso le stazioni autostradali (in alcuni casi, trascorrono anche dieci giorni dal momento del versamento del denaro da parte del personale di esazione o del cliente presso le casse self-service), sia soprattutto dei tempi necessari ad altra società che, per conto della concessionaria di Anas, una volta prelevato l'incasso, effettua il servizio di conteggio e rendicontazione del denaro, anche in vista dell'espletamento di indagini giudiziarie che dovessero rendersi necessarie in caso di illeciti accertati dopo le 24 ore dall'esazione dei pedaggi (art. 11, comma 1, lett. *d*) ed *e*), del Codice) (provv. 17 novembre 2011 [doc. *web* n. 1877929]).

Di altri provvedimenti relativi alla videosorveglianza si da conto nel paragrafo 10.1.1.

12. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Particolarmente intensa nel 2011 è stata l'attività del Garante nel settore dei trasferimenti transfrontalieri di dati personali attraverso il rilascio sia di autorizzazioni ad hoc in materia di *Binding Corporate Rules - BCR* (norme vincolanti di impresa), sia di autorizzazioni di carattere generale, volte ad attuare alcune decisioni della Commissione europea in merito all'adeguatezza della normativa di protezione dei dati offerta da un Paese non appartenente all'Unione europea (decisione di cui all'art. 25, paragrafi 1 e 2, della Direttiva n. 95/46/CE).

Con riferimento alle *BCR*, l'Autorità, con i provvedimenti del 5 maggio 2011 [doc. *web* n. 1829762] e dell'11 ottobre 2011 [doc. *web* n. 1849957], si è pronunciata in ordine allo schema di norme vincolanti d'impresa elaborato da un'importante gruppo societario di carattere multinazionale operante nel settore della produzione di pneumatici.

Al Garante sono pervenute due istanze di autorizzazione al trasferimento di dati personali verso Paesi terzi relative al medesimo progetto di *BCR*, approvato a seguito della conclusione di una procedura di cooperazione europea coordinata dalla *Commission nationale de l'informatique et des libertés* (Autorità francese in materia di protezione dei dati) ai sensi del sistema di mutuo riconoscimento, volto a semplificare l'esame degli schemi predisposti dalle società (v. Relazione 2009, p. 189).

La prima richiesta di autorizzazione è stata presentata da una società per azioni, filiale italiana del gruppo multinazionale sopra indicato, con riferimento ai trasferimenti verso le altre filiali del gruppo con sede in Paesi non appartenenti all'Unione europea. L'istanza aveva ad oggetto i trasferimenti dei dati personali relativi: ai dipendenti e ai candidati all'assunzione, per finalità connesse rispettivamente alla gestione del rapporto di lavoro e del processo di selezione; ai fornitori e ai clienti, per finalità amministrativo contabili inerenti al rapporto contrattuale; ai consumatori, per rispondere a richieste di informazioni o a reclami; ai giornalisti, per la trasmissione di comunicati stampa o di inviti ad eventi promozionali.

Il Garante, a seguito di una complessa istruttoria, nel corso della quale ha preso atto delle dichiarazioni integrative rese dalla richiedente Autorità (relative, in particolare, all'efficacia vincolante dell'accordo intra-gruppo con cui le filiali si impegnano al rispetto delle norme

vincolanti d'impresa, all'esatta indicazione dei dati trasferiti e delle finalità dei trasferimenti e all'obbligo di rilascio di idonea informativa agli interessati), ha autorizzato il trasferimento summenzionato secondo le modalità fissate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate. Il Garante ha comunque ribadito il proprio potere di svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, eventuali provvedimenti di blocco o di divieto. Infine, ha precisato che le operazioni di trattamento dei dati personali, anche se poste in essere a seguito del rilascio dell'autorizzazione, sono lecite solo ove conformi alla normativa nazionale vigente e alle sue successive modificazioni, anche in materia di protezione dei dati personali, con particolare riferimento alle specifiche disposizioni sui presupposti di legittimità delle attività di raccolta dei dati oggetto del trasferimento e sulla sussistenza dei presupposti di legittimità per la comunicazione dei dati medesimi.

Nel secondo caso, l'istanza di autorizzazione è stata presentata da una fondazione, stabilita in Italia e appartenente al medesimo gruppo multinazionale d'impresa, al fine di ottenere l'autorizzazione del Garante ai trasferimenti infragruppo tramite *BCR* verso altre filiali stabilite in Paesi terzi e relativamente ai soli dati personali dei clienti trasferiti, per finalità amministrativo contabili inerenti al rapporto contrattuale.

Anche in questa ipotesi, il Garante ha effettuato una complessa istruttoria, chiedendo opportuni chiarimenti in merito all'individuazione dei soggetti coinvolti nel trasferimento transfrontaliero dei dati personali e all'effettiva conclusione, da parte della fondazione summenzionata, dell'accordo infragruppo con cui si garantisce efficacia vincolante alle *BCR*.

L'autorizzazione è stata rilasciata nei limiti delle modalità di trasferimento indicate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate.

In termini più generali nel 2011 si è notevolmente ampliato il numero dei Paesi non appartenenti all'Unione europea considerati adeguati ai sensi dell'art. 25, paragrafi 1 e 2 della Direttiva n. 95/46/CE, per il livello di protezione dei dati personali da essi fornito.

Questa Autorità ha, infatti, recepito con proprie autorizzazioni generali le decisioni della Commissione europea in merito all'adeguatezza delle normative di protezione dei dati

personali del Principato di Andorra (autorizzazione 3 febbraio 2011 [doc. *web* n. 1788981]; delle Isole Fær Øer (autorizzazione 7 settembre 2011 [doc. *web* n. 1838283]); del Baliato di Jersey (autorizzazione 7 settembre 2011 [doc. *web* n. 1838359]) e dello Stato di Israele (autorizzazione 20 gennaio 2012 [doc. *web* n. 1868817]).

In questo modo si consente ai titolari stabiliti nel territorio dello Stato italiano di trasferire dati personali verso uno dei Paesi oggetto dell'autorizzazione senza l'adempimento di ulteriori formalità (quali ad es. clausole contrattuali tipo, *BCR*, autorizzazioni *ad hoc*).

Nell'autorizzare tali trasferimenti, l'Autorità si è riservata di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento.

Trasferimento di dati personali in Argentina

Il Ministero degli affari esteri ha richiesto la collaborazione del Garante per dare attuazione al *Memorandum* di intesa fra l'Italia e l'Argentina firmato il 1° giugno 2011 ai fini del trasferimento alle autorità argentine di documentazioni d'archivio, custodite presso la rete diplomatico-consolare italiana in Argentina, concernenti le vittime della dittatura militare (1976-1983). Tale collaborazione è avvenuta nell'ambito dei lavori della commissione tecnica bilaterale appositamente istituita, nel corso dei quali le autorità argentine hanno dichiarato che le finalità della richiesta della documentazione riguardavano la ricostruzione del periodo storico degli anni della dittatura. In particolare, in tale occasione è stato stabilito che copia ufficiale della documentazione custodita negli archivi consolari relativa a cittadini italiani, doppi cittadini o cittadini di origine italiana, vittime del regime militare argentino, sarebbe stata consegnata all'Archivio nazionale della memoria che l'avrebbe utilizzata esclusivamente per i propri fini istituzionali, stabiliti con il decreto della Repubblica Argentina, n. 1259/2003, in conformità alla vigente normativa argentina sulla protezione dei dati personali, nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate.

In seguito, il Ministero degli affari esteri, nell'illustrare formalmente al Garante il contenuto dei lavori della commissione, attesa l'impossibilità di comunicare singolarmente agli interessati l'imminente trasferimento della predetta documentazione, ha rappresentato l'intenzione di informare adeguatamente e tempestivamente gli interessati in Italia e presso la

collettività argentina attraverso un'apposita informativa (di cui ha fornito copia), da pubblicare nei due mesi antecedenti alla prima consegna del materiale e nei quattro mesi successivi sul proprio sito istituzionale, nonché su quelli dell'Ambasciata d'Italia a Buenos Aires e dei Consolati dipendenti, e da divulgare attraverso i canali consolari. Il Ministero degli affari esteri ha, inoltre, precisato che la consegna della copia della documentazione all'Archivio della memoria avverrà gradualmente, in plico chiuso sigillato, dopo aver espletato, ove necessario, le procedure previste dalla normativa in vigore in materia di utilizzo di documentazione classificata.

Con il provvedimento del 25 gennaio 2012 [doc. *web* n. 1872111], il Garante, sulla base della propria autorizzazione del 9 giugno 2005, relativa al trasferimento dei dati personali verso l'Argentina (adottata in conformità alla decisione della Commissione europea del 30 giugno 2003, n. 2003/490/CE, con la quale è stato considerato adeguato il livello di protezione dei dati personali offerto dalle disposizioni di rango costituzionale e dalle altre norme vigenti in Argentina), ha ritenuto che il trasferimento dei dati personali contenuti nella documentazione in parola non fosse contrastante con il Codice e che le garanzie individuate dal Ministero degli affari esteri e dalla commissione tecnica bilaterale fossero idonee ad assicurare il rispetto dei diritti degli interessati.

13. LIBERE PROFESSIONI

13.1. ATTIVITÀ FORENSE E INVESTIGATIVA

Nel corso del 2011 sono pervenute all'Autorità alcune segnalazioni relative al trattamento di dati personali nell'ambito dell'attività forense e investigativa.

Trattamento dati per fare valere un diritto in sede giudiziaria

Con una segnalazione è stato lamentato che un avvocato aveva allegato un provvedimento giudiziale contenente dati personali del segnalante alla richiesta rivolta all'anagrafe di un comune di verificare la residenza dell'interessato stesso.

Il Garante ha rilevato che il trattamento dei dati del segnalante è stato effettuato *"per far valere o difendere un diritto in sede giudiziaria"*, finalità che ricorre anche quando i dati sono trattati nel corso di un procedimento amministrativo (quale l'accertamento della residenza da parte dell'anagrafe comunale) e nella fase propedeutica all'instaurazione di un eventuale giudizio. In relazione a tale finalità, l'informativa all'interessato e il suo consenso non sono richiesti (artt. 13, comma 5, lett. *b*), e 24, comma 1, lett. *f*), del Codice) ed anche i dati sensibili possono essere trattati senza consenso, previa autorizzazione del Garante (art. 26, comma 4, lett. *c*), del Codice; v. autorizzazione n. 4/2011 al trattamento dei dati sensibili da parte dei liberi professionisti del 24 giugno 2011 [doc. *web* n. 1822597]).

Alla luce delle disposizioni citate, il trattamento dei dati effettuato dall'avvocato è risultato, pertanto, lecito (nota 26 ottobre 2011).

L'Autorità si è espressa nello stesso senso in un caso in cui il trattamento dei dati personali del segnalante era avvenuto tramite una e-mail spedita dall'avvocato della controparte precedentemente all'avvio di un contenzioso in sede giudiziaria (nota 27 dicembre 2011).

Attività investigative

In risposta ad un quesito presentato da un investigatore privato, concernente la legittimità della raccolta di dati personali nell'ambito di un'attività finalizzata all'accertamento di eventuali frodi assicurative, il Garante ha evidenziato che per far valere o difendere un diritto in sede giudiziaria l'investigatore risulta legittimato a presentare la richiesta di accesso ai dati, con esonero dagli adempimenti dell'informativa e del consenso, sempre che i dati siano trattati esclusivamente per la finalità citata e per il periodo strettamente necessario al suo perseguimento (cfr. art. 9 del codice di deontologia e di buona condotta per i trattamenti di