finanziamento. Tali segnalazioni sarebbero state "*abusive in quanto non corrispondenti ad alcuna richiesta di concessione di fido da parte delle due società*".

Dai riscontri forniti dalle menzionate società è emerso che, in un caso, la finanziaria aveva ricevuto una richiesta per una operazione di *leasing* da una persona incaricata dalla stessa società segnalante, alla quale, secondo quanto dichiarato dalla finanziaria era stata fornita in forma orale la necessaria informativa. Nell'altro caso invece, è risultato che la finanziaria aveva ricevuto i dati da un'altra società e non era stata data l'informativa ai sensi dell'art. 13 del Codice in merito alla comunicazione dei dati a terzi. All'esito dell'attività istruttoria il Garante, come in precedenti pronunce, ha confermato che la comunicazione dei dati alla Centrale dei rischi di Banca d'Italia, in quanto prevista da una normativa, non richiede il rilascio del consenso da parte degli interessati (art. 24, comma 1, lett. *a*), del Codice). Ha poi precisato che l'informativa deve essere fornita quando i dati sono raccolti direttamente presso gli interessati indicando anche "*i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati*", e che il titolare del trattamento non è tenuto a fornire la predetta informativa ove essi siano raccolti presso terzi e "*trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria*" (art. 13, comma 5, lett. *a*), del Codice).

Il Garante ha pertanto prescritto alla società che ha raccolto i dati dall'interessato e comunicato gli stessi alla finanziaria, di predisporre un'informativa in stretta aderenza a quanto previsto dall'art. 13 del Codice, nella quale sia riportata anche l'indicazione dei soggetti terzi ai quali i dati dei clienti potranno essere comunicati, riservando ad un autonomo procedimento le valutazioni di competenza in ordine all'eventuale applicazioni di sanzioni amministrative (*Provv.* 10 novembre 2010 [doc. *web* n. 1769502]).

11.3. SETTORE ASSICURATIVO

In ambito assicurativo, si menziona una segnalazione avente ad oggetto il trattamento di dati personali effettuato per il servizio di fornitura telefonica di preventivi.

L'istante aveva lamentato che l'operatrice del *call center* cui si era rivolto per ricevere un preventivo in ordine a una polizza assicurativa concernente la responsabilità civile

derivante dalla circolazione di veicoli a motore non aveva provveduto, successivamente al rilascio del preventivo, a cancellare i suoi dati personali forniti in occasione del contatto telefonico.

Il Garante ha ritenuto lecita, anche ai fini di una eventuale tutela degli operatori telefonici, l'acquisizione dei dati identificativi dell'interlocutore, utili altresì a consentire una reale "personalizzazione" del preventivo; ciò, tra l'altro, in osservanza di specifiche disposizioni legislative (art. 131 del d.lgs. 7 settembre 2005, n. 209) e regolamentari (artt. 5 e 7, regolamento ISVAP 9 maggio 2008, n. 23). È risultata inoltre giustificata l'acquisizione dei recapiti degli utenti nella misura in cui gli interessati abbiano espressamente manifestato la propria volontà di ricevere il preventivo per iscritto.

Per contro, l'Autorità ha ritenuto sproporzionata (art. 11, comma 1, lett. *d*), del Codice) l'acquisizione di altri dati da parte della compagnia, non essendone stata provata l'effettiva necessità e non eccedenza in relazione alla finalità concretamente perseguita; ciò, tenuto anche conto che la medesima compagnia avrebbe potuto, in astratto, ricorrere a locuzioni più generiche, parimenti idonee a consentire una puntuale valutazione del rischio, ma meno lesive dei princìpi di protezione dei dati.

Il Garante ha quindi disposto nei confronti della compagnia il blocco dell'ulteriore trattamento di tali dati nell'espletamento del servizio di fornitura telefonica di preventivi, prescrivendo al contempo la cancellazione di quelli relativi agli utenti per i quali non fossero stati completati i preventivi, la cui conservazione non è risultata giustificata in relazione alle esigenze prospettate dalla compagnia (art. 11, comma 1, lett. *e*), del Codice; *Provv.* 2 dicembre 2010 [doc. *web* n. 1780277]).

11.4. RAPPORTI DI LAVORO E PREVIDENZA

11.4.1. Rapporto di lavoro in ambito pubblico

Anche nel 2010, per dare riscontro a molteplici segnalazioni e quesiti di amministrazioni pubbliche, dipendenti e organizzazioni sindacali, sono state richiamate le "*Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*" (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In merito ad una richiesta di un'organizzazione sindacale di conoscere i nominativi del personale che aveva partecipato ad attività ispettive, il numero delle ispezioni ed i relativi corrispettivi, l'Ufficio ha ribadito che, salve puntuali previsioni normative o contrattuali, l'amministrazione può fornire alle oo.ss. solo dati numerici o aggregati (art. 19, comma 3, del Codice; punto 5.2. del cit. *provvedimento*) (*Nota* 12 aprile 2010).

In questi casi, come evidenziato dall'Ufficio in risposta ad un quesito riguardante l'accesso delle RSU alla documentazione concernente i debiti e i crediti orari, nonché i tabulati delle timbrature del personale amministrativo di una scuola, spetta all'amministrazione destinataria della richiesta valutare la sussistenza dell'interesse giuridicamente rilevante e le altre condizioni che legittimano l'accesso del richiedente, nonché le ragioni per le quali tali documenti possono essere sottratti alla sua conoscibilità, essendo l'amministrazione in possesso di tutti gli elementi di ponderazione necessari (*Nota* 21 aprile 2010).

Con riferimento alla segnalazione dell'avvenuta pubblicazione, su un periodico informativo di un comune, di alcuni dati personali dei singoli dipendenti dell'ente locale, riguardanti il rapporto di lavoro e lo stato di salute (tra cui trattamento economico, trattenute previdenziali, giorni di ferie, di malattia, permessi usufruiti ai sensi della l. n. 104/1992, assenze retribuite per maternità, congedo parentale e malattia figli), l'Ufficio ha evidenziato, in particolare, il divieto di diffondere dati idonei a rivelare lo stato di salute. Il Comune ha, al riguardo, assicurato che le future pubblicazioni sul proprio periodico saranno effettuate in conformità al vigente quadro normativo (art. 21, comma 1, l. 18 giugno 2009, n. 69; v. ora anche il comma 1-*bis*, introdotto dall'art. 5, comma 2, l. 4 novembre 2010, n. 183) (*Nota* 24 novembre 2010).

Sempre in materia di dati sensibili, in ottemperanza al *provvedimento* 21 ottobre 2009 [doc. *web* n. 1689440] (v. *Relazione* 2009, p. 164), il Ministero della difesa-Direzione generale per il personale militare ha adottato il 2 dicembre 2009 un decreto dirigenziale che, in particolare, dispone la cancellazione dalla documentazione sanitaria delle informazioni sullo stato di salute del personale, ad esclusione del giudizio medico-legale di idoneità al servizio, della riconducibilità dell'infermità a causa di servizio, della posizione di collocamento in congedo e dell'abilità a determinati impieghi. Più in generale, il

decreto vieta il trattamento di dati relativi allo stato di salute del personale che non siano indispensabili all'adozione dei provvedimenti di competenza.

Sono stati avviati dal Ministero della difesa approfondimenti, anche sulla base di indicazioni rese per le vie brevi dal Garante, in relazione alla prassi di comunicare all'autorità di pubblica sicurezza i nominativi dei militari affetti da patologie psiconeurologiche ai fini della revoca dell'autorizzazione di polizia a detenere armi a titolo privato.

Su eventuali proposte di modifica della normativa sull'ordinamento militare dovrà esprimersi l'Autorità ai sensi dell'art. 154, comma 4, del Codice (d.P.R. 15 marzo 2010, n. 90) (*Nota* 30 settembre 2010).

In argomento, si segnala da ultimo il d.lgs. 26 ottobre 2010, n. 204 il quale prevede che con decreto adottato dal Ministro della salute, di concerto con il Ministro dell'interno, sentito il Garante per la protezione dei dati personali, siano definite "*le modalità dello scambio protetto dei dati informatizzati tra il servizio sanitario nazionale e gli uffici delle forze dell'ordine nei procedimenti finalizzati all'acquisizione, alla detenzione ed al conseguimento di qualunque licenza di porto delle armi*" (art. 6).

A seguito di una segnalazione riguardante un bando di concorso del Ministero della difesa per allievi dell'Accademia navale, il quale aveva previsto l'esclusione dal concorso dei concorrenti al Corpo sanitario militare marittimo in caso di positività al *test HIV*, l'Ufficio ha avviato una serie di approfondimenti nei confronti dell'amministrazione della difesa per verificare le particolari cautele in materia di indagini volte ad accertare l'esistenza la sieropositività nei confronti di persone prese in considerazione per l'instaurazione di un rapporto di lavoro (artt. 5 e 6, l. 5 giugno 1990, n. 135; Corte costituzionale sentenza n. 218 del 1994; artt. 3, 11, 22, 112 e 184, comma 3, del Codice) (*Nota* 8 gennaio 2010).

Sono pervenute, inoltre, all'Autorità numerose segnalazioni riguardanti l'affidabilità degli strumenti telematici utilizzati dal Ministero per i beni e le attività culturali per la raccolta delle domande di partecipazione ad una procedura selettiva per restauratori e per l'iscrizione ad un elenco riguardante talune categorie di archeologi. Al riguardo il citato Ministero ha fornito idonee assicurazioni sulle misure adottate per garantire la protezione

dei dati personali raccolti, con particolare riferimento all'affidabilità dei siti Internet utilizzati (*Nota* 30 settembre 2010).

In un altro caso alcuni dipendenti hanno lamentato la pubblicazione, sul sito del Ministero della giustizia di alcuni provvedimenti, relativi all'inquadramento del personale e contenenti, tra l'altro, i codici fiscali dei dipendenti, accessibili anche tramite i comuni motori di ricerca. In proposito il Ministero ha dichiarato di aver effettuato la pubblicazione in ottemperanza a quanto previsto dall'art. 32 della l. 18 giugno 2009, n. 69 e di aver provveduto a cancellare i codici fiscali (*Nota* 10 novembre 2010).

11.4.2. Rapporto di lavoro in ambito privato

In una segnalazione un dipendente di una società aveva ritenuto illecita la richiesta che quest'ultima gli aveva rivolto di documentare (dal punto di vista sanitario) le "*improcrastinabili esigenze personali*" poste a fondamento dell'istanza di fruizione di un periodo feriale.

L'Autorità ha ritenuto ingiustificata la richiesta di documentazione in quanto, benché formulata nell'ambito di una legittima attività di verifica per finalità di gestione del rapporto di lavoro, non trovava giustificazione né nella normativa vigente (art. 2109 c.c.), né nella normativa contrattuale esaminata. Peraltro, la stessa richiesta non è risultata giustificata nemmeno in relazione alla finalità concretamente perseguita dalla società, tenuto conto della discrezionalità che la stessa normativa riconosce a quest'ultima nell'individuare il periodo di fruizione delle ferie da parte dei lavoratori (art. 2109 c.c.; art. 38 del CCNL applicabile).

Conseguentemente, è stato prescritto alla società di sensibilizzare i soggetti preposti a non chiedere la produzione di documenti volti a rendere note le ragioni delle richieste di congedo ordinario avanzate dai dipendenti (*Provv.* 4 novembre 2010 [doc. *web* n. 1779735]).

L'Autorità ha poi esaminato una richiesta di verifica preliminare formulata da una società (anche nell'interesse di altre controllate) che intendeva adottare uno strumento di valutazione dei dipendenti basato su procedure di autovalutazione e sui riscontri forniti dai terzi.

Il sistema, preordinato all'elaborazione dei dati acquisiti per il tramite di questionari compilati in forma anonima (successivamente "sintetizzati" e "aggregati" in *report* finali resi disponibili, tra l'altro, agli stessi interessati), sarebbe stato utilizzato su un numero ristretto di dipendenti (circa una ventina su base annua), anche in collegamento con il processo di valutazione del personale e per la corresponsione di eventuali incentivi economici. Inoltre, tale sistema avrebbe consentito ai lavoratori di valutare meglio le proprie capacità professionali e l'attività espletata, con significativi contributi al miglioramento delle prestazioni lavorative e al raggiungimento degli obiettivi concordati in sede aziendale. L'Autorità ha reputato il trattamento lecito e proporzionato, sia perché giustificato dalle specifiche dinamiche di tipo contrattuale presenti in ambito aziendale, sia perché effettuato su base meramente consensuale (art. 23 del Codice), senza pregiudizio per i lavoratori che avessero manifestato un eventuale diniego al trattamento, della possibilità di conseguire comunque un incentivo di natura economica.

L'Autorità ha tuttavia richiamato al rispetto di specifiche disposizioni (art. 14 del Codice; art. 8 della l. n. 300/1970), prescrivendo al contempo alla società di conservare i dati non oltre il termine strettamente necessario al perseguimento della finalità dichiarata (art. 11, comma 1, lett. *e*), del Codice) (*Provv.* 4 novembre 2010 [doc. *web* n. 1771838]).

A seguito di una segnalazione l'Autorità si è poi pronunciata sul trattamento di dati personali dei lavoratori svolto da una società mediante sistemi di localizzazione satellitare (*Provv.* 7 ottobre 2010 [doc. *web* n. 1763071]).

L'interessato aveva lamentato l'installazione, a bordo di alcuni autoveicoli in dotazione alla società presso la quale prestava servizio, di un sistema di localizzazione satellitare in assenza di preventiva informativa ai lavoratori e in asserita violazione della disciplina sul controllo a distanza dell'attività dei lavoratori (art. 4, comma 2, l. n. 300/1970).

L'Autorità, nel riconoscere che i dispositivi in esame servivano anche per pianificare gli interventi, diminuire i costi per danni conseguenti a violazioni del codice della strada, nonché per determinare i costi di trasferta e di intervento, e per esigenze di sicurezza sul lavoro, ha tuttavia evidenziato che il loro impiego deve comunque avvenire, oltre che in osservanza della pertinente disciplina di settore in tema di controlli a distanza, nel rispetto

dei princìpi in materia di protezione dei dati personali e con modalità concretamente idonee a garantire, in particolare, l'osservanza dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2 del Codice).

Le risultanze istruttorie hanno evidenziato che la società non aveva rispettato il precetto di cui all'art. 4, comma 2, della l. n. 300/1970; non aveva notificato il trattamento, né documentato la formale designazione quali incaricati del trattamento dei soggetti effettivamente legittimati ad accedere alle informazioni acquisite (art. 30 del Codice).

L'Autorità ha quindi disposto il blocco del trattamento nei confronti della società titolare; formulato al contempo –in caso di eventuale rilascio del provvedimento autorizzatorio da parte del competente ufficio territoriale del Ministero– specifiche prescrizioni in tema di notificazione del trattamento e di designazione degli incaricati, e infine, ha invitato la società commisurare i tempi di conservazione dei dati alle finalità concretamente perseguite.

Il trattamento dei dati personali dei dipendenti effettuato mediante strumenti di localizzazione satellitare è stato anche oggetto di una verifica preliminare richiesta da un'associazione operante nel campo dei controlli sulle aziende zootecniche per certificare l'effettività dei controlli svolti presso le aziende associate (in ottemperanza alle pertinenti normative di settore), e documentare la propria attività presso gli enti pubblici sovvenzionanti (in particolare, il Ministero delle politiche agricole, alimentari e forestali).

Il Garante ha ritenuto lecito il trattamento ove effettuato per la finalità dichiarata e nel rispetto delle prescrizioni di cui all'art. 4, comma 2, l. n. 300/1970; ha prescritto all'associazione di anonimizzare i dati di localizzazione in caso di loro comunicazione a terzi per dar conto dell'attività espletata, nonché di rendere agli interessati un'informativa dettagliata ed esaustiva circa il trattamento da svolgere. È stato infine prescritto all'associazione di provvedere alla notifica del trattamento (*Provv.* 18 febbraio 2010 [doc. *web* n. 1703103]).

A seguito di alcune notizie di stampa, l'Autorità ha valutato i trattamenti svolti da una società in relazione ai dati personali dei propri dipendenti, consistenti nell'utilizzo di "tagliandi" scritti a fini di allontanamento temporaneo dalla postazione di lavoro, per

assicurare al cliente una fornitura di prodotti continua e per garantire una efficace e tempestiva sostituzione dei dipendenti momentaneamente allontanatisi.

Il trattamento è stato tuttavia ritenuto lesivo della disciplina in materia di protezione dei dati personali ed è stato vietato alla società di trattare ulteriormente i dati dei lavoratori acquisiti per il tramite dei citati tagliandi scritti.

Al riguardo, il Garante ha rilevato che l'utilizzo dei tagliandi, per allontanamenti dei lavoratori dovuti all'espletamento di necessità "fisiologiche", risulta contrario all'art. 2 del Codice, soprattutto in considerazione del potenziale condizionamento (anche in termini di mortificazione personale) degli interessati in ordine alla propria libertà di movimento, nonché comunque sproporzionato e non necessario (artt. 3 e 11, comma 1, lett. *d*), del Codice).

Nel vietare il trattamento l'Autorità ha inoltre prescritto alla società di predisporre nuove modalità di comunicazione delle assenze temporanee dei dipendenti dalla propria postazione lavorativa, tali da assicurare l'effettiva salvaguardia della dignità e riservatezza dei lavoratori (*Provv.* 24 febbraio 2010 [doc. *web* n. 1705070]).

Cessione d'azienda: uso della casella di posta dell'ex dipendente

Con il *provvedimento* 22 aprile 2010 [doc. *web* n. 1727692], il Garante si è occupato di una particolare fattispecie: la cessione inter-societaria dell'azienda e, per quanto di competenza dell'Autorità, degli *account* di posta elettronica appartenenti al dominio aziendale.

Nel caso, due lavoratrici hanno lamentato l'utilizzo da parte della società, acquirente del compendio fallimentare, degli indirizzi di posta elettronica aziendale loro assegnati.

In particolare, le segnalanti hanno evidenziato la possibilità che la società subentrante non avesse disattivato i rispettivi *account* di posta elettronica (dal momento che le comunicazioni inviate non generavano messaggi di errore) rappresentando quindi il rischio che la suddetta società potesse leggere le e-mail pervenute sui propri indirizzi.

La società ha ammesso di utilizzare le caselle di posta elettronica delle segnalanti, precisando di aver adottato la modalità "*catch-all*", tale da consentire la ricezione di tutti i messaggi pervenuti sugli indirizzi appartenenti al dominio aziendale in maniera indifferenziata su un'unica casella di posta elettronica.

La società ha sottolineato che tale scelta era stata giustificata dalla circostanza dell'avvenuto acquisto dell'intero compendio fallimentare della società cedente, incluso il

relativo avviamento e, quindi, anche il dominio aziendale, ivi compresi gli indirizzi di posta elettronica aziendale, nonché dalla circostanza che l'utilizzo di questi ultimi risultasse indispensabile alla corretta gestione dei rapporti commerciali della società.

Ciò in considerazione del fatto che le segnalanti avrebbero svolto, anche successivamente alla cessione aziendale, un'attività di sviamento della clientela.

La società ha rappresentato altresì come le segnalanti risultassero socie di una nuova società, dalla denominazione simile a quella della società cedente, costituita poco dopo la dichiarazione di fallimento.

Il Tribunale di Bologna, adito sulla questione, aveva dato atto che la ricezione dei dati da parte della stessa avveniva in modo indifferenziato secondo il *cd.* "sistema del *catch-all*", che non consentiva di risalire al destinatario, e che inoltre le caselle in questione erano di pertinenza aziendale con conseguente proprietà delle stesse da parte dell'imprenditore e possibilità dello stesso di accedervi.

Il Garante, tuttavia, considerando l'esigenza di tutela dei dati personali in rilievo, con il citato *provvedimento*, ha prescritto alla società subentrata nella titolarità degli indirizzi in questione la disattivazione di tutti gli *account*, appartenenti al dominio aziendale, ma attribuiti personalmente a soggetti che non facevano più parte dell'organizzazione imprenditoriale della società e la predisposizione di un sistema idoneo ad informare della disattivazione tutti i mittenti di comunicazioni inviate agli *account*, invitando all'inoltro della corrispondenza di lavoro ad un indirizzo di posta elettronica alternativo.

11.4.3. Previdenza

Un cittadino aveva segnalato al Garante di aver ricevuto dall'INPS un plico che presentava, sulla parte esterna, indicazioni relative alla copia, ivi contenuta, di un verbale di accertamento dell'invalidità civile. Al riguardo, l'Ufficio ha evidenziato che i plichi postali non devono recare, sulla parte esterna, indicazioni da cui possano evincersi, in modo esplicito, informazioni idonee a rivelare lo stato di salute dell'interessato (artt. 11 e 22, comma 3, del Codice) (*Nota* 23 luglio 2010).

Nel corso del 2010 sono proseguite le attività di controllo avviate nell'anno precedente

sui sistemi informativi dell'INPS. In particolare, gli approfondimenti ispettivi hanno riguardato la conformità alla disciplina sulla protezione dei dati personali degli accessi alle banche dati dell'Istituto effettuati da soggetti esterni, specie in relazione alle finalità istituzionali perseguite, alle tipologie di dati trattati e alle modalità di trattamento. All'esito di taluni accertamenti effettuati *in loco* sui sistemi informativi dell'INPS, a seguito di controlli avviati negli anni precedenti, l'Ufficio ha chiesto all'Istituto informazioni relative: ai sistemi di autenticazione ed autorizzazione degli applicativi utilizzati dai soggetti esterni; al sistema di gestione telematica della procedura di riconoscimento dei benefici in materia di invalidità civile, cecità civile, sordità civile, *handicap* e disabilità; alle modalità di comunicazione all'Istituto delle variazioni anagrafiche da parte degli enti locali; al funzionamento del "casellario pensioni" e alla banca dati contenente le attestazioni ISEE (*Nota* 23 dicembre 2010).

Una direzione provinciale dell'INPS ha informato l'Autorità, ai sensi degli artt. 19 e 39 del Codice, di voler trasmettere ad un istituto autonomo case popolari i dati personali relativi agli importi delle pensioni e degli assegni sociali erogati dall'INPS in favore dei componenti i nuclei familiari assegnatari di alloggi, per consentire allo stesso IACP di verificare le autocertificazioni degli interessati sulla loro situazione reddituale. Al riguardo l'Ufficio ha rappresentato che, in particolare, ove il flusso di dati personali trovi la propria fonte nelle norme che impongono di controllare la veridicità delle dichiarazioni sostitutive, non occorre effettuare alcuna comunicazione al Garante. Ciò fermo restando il rispetto dei princìpi di pertinenza e non eccedenza dei dati oggetto di comunicazione, nonché delle modalità e dei limiti dei controlli stabiliti dalle medesime disposizioni (art. 11, comma 1, lett. *d*), del Codice e artt. 43, 46 e 71 del d.P.R. 28 dicembre 2000, n. 445) (*Nota* 28 gennaio 2010).

In relazione ad un progetto finalizzato all'assistenza di lavoratori esposti all'amianto, l'INPS ha comunicato all'Autorità, ai sensi dell'art. 39 del Codice, di voler trasmettere ad un'azienda sanitaria della Regione Friuli Venezia Giulia taluni dati personali relativi agli occupati in aziende operanti in determinate zone del territorio regionale. Al riguardo, l'Ufficio ha evidenziato che la speciale disciplina prevista dall'art. 39 del

Codice riguarda esclusivamente comunicazioni di dati non sensibili. La comunicazione prospettata dall'INPS può, dunque, essere effettuata soltanto nella misura in cui non si tratti di dati idonei a rivelare lo stato di salute degli interessati (quali, ad es., quelli riguardanti i lavoratori esposti richiedenti il riconoscimento dei benefici connessi a tale esposizione ai sensi dell'art. 13 della l. 27 marzo 1992, n. 257 oppure il riconoscimento di malattie professionali). Con riferimento, inoltre, alla prospettata interconnessione dei suddetti dati con ulteriori informazioni, anche di carattere sensibile detenute da altri soggetti pubblici, l'Ufficio ha evidenziato la necessità di individuare con chiarezza le finalità perseguite, di verificare l'esistenza di idonei presupposti giuridici (artt. 20 e 22, comma 11, del Codice) e di rispettare il pertinente quadro normativo di settore (art. 244, d.lgs. 9 aprile 2008, n. 81; d.P.C.m. 10 dicembre 2002, n. 308; l.r. 12 settembre 2001, n. 22) (*Nota* 10 dicembre 2010).

11.5. ALTRE ATTIVITÀ IMPRENDITORIALI

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

Per facilitare la consultazione dei dati degli iscritti nelle graduatorie ad esaurimento del personale docente pubblicate sui siti *web* degli uffici scolastici provinciali del Ministero della pubblica istruzione, una società ha chiesto al Garante di essere esonerata dall'obbligo di rendere l'informativa.

Il Garante ha accolto l'istanza di esonero formulata dalla società per la ritenuta impossibilità di rilasciare l'informativa individuale a tutti gli interessati (pari a circa 300.000 unità), nonché in considerazione dell'utilità sociale rivestita dal progetto e delle specifiche previsioni in materia (che facoltizzano i soggetti privati, nei termini e alle condizioni ivi previste, a riutilizzare le informazioni del settore pubblico per finalità anche commerciali; art. 2, comma 1, lett. *e*), del d.lgs. n. 24 gennaio 2006, n. 36).

L'Autorità ha comunque prescritto alla società di pubblicare sul proprio sito *web* un'idonea e preventiva informativa a vantaggio di tutti i docenti interessati, dalla quale emergano le puntuali caratteristiche del trattamento effettuato in ordine ai loro dati personali (*Provv.* 26 marzo 2010 [doc. *web* n. 1721169]).

In un altro caso, l'Autorità è stata chiamata a pronunciarsi sul trattamento effettuato da una società relativamente alle richieste di assistenza formulate dagli utenti per il tramite del relativo *call center*.

Il segnalante, in particolare, aveva lamentato che la società cui si era rivolto per ricevere informazioni generiche sui centri di assistenza autorizzati alla riparazione della sua stampante subordinava il rilascio di dette informazioni alla preventiva acquisizione dei dati personali del chiamante e al rilascio del consenso al relativo trattamento.

Al riguardo, l'Autorità ha ritenuto sproporzionata l'acquisizione di dati personali diversi dal nome e cognome del chiamante nella fase antecedente l'intervento di assistenza telefonica, talora, in astratto, potenzialmente risolutivo del problema. Viceversa, la raccolta di altri dati (indirizzo; numero di telefono; indirizzo di posta elettronica) è stata ritenuta lecita se effettuata in un momento successivo, qualora si dovesse rendere necessaria la predisposizione di misure alternative all'assistenza telefonica (ad. es, per l'organizzazione di interventi a domicilio).

L'Autorità ha pertanto vietato alla società di trattare ulteriormente i predetti dati nella fase antecedente l'intervento di assistenza tecnica (*Provv.* 4 marzo 2010 [doc. *web* n. 1721214]).

Una volontaria *Caritas* aveva segnalato all'Autorità che, accompagnando una portatrice di *handicap* a fare la spesa presso un punto vendita di una nota catena commerciale di supermercati, aveva constatato che per il servizio di consegna a domicilio gratuito riservato agli invalidi al 100%, veniva richiesta copia del verbale di invalidità, tanto che un'addetta all'esercizio commerciale aveva rifiutato all'interessata di poter fruire del servizio sulla base della mera esibizione di una tessera attestante lo stato di invalidità, affermando che, al contrario, era indispensabile acquisire copia del predetto verbale.

Il Garante ha reputato sproporzionata la richiesta di esibire copia del verbale rilasciato, tenuto conto della pluralità di informazioni in esso contenute e, in particolare, del giudizio diagnostico espresso dalla Commissione medica. L'Autorità ha pertanto vietato ulteriori richieste di esibizione del verbale e ha invitato la società a riformulare l'informativa resa alla clientela interessata alla tipologia di trattamenti in esame, carente

di talune indicazioni richieste dall'art. 13 del Codice (*Provv.* 13 maggio 2010 [doc. *web* n. 1729156]).

A seguito di un procedimento su ricorso, l'Autorità si è poi pronunciata sul trattamento di dati personali effettuato da una società di autonoleggio.

Dalla documentazione acquisita era emerso che la società, nell'ambito di un contratto stipulato con l'interessato, aveva comunicato alcuni suoi dati personali ad altra società (proprietaria del veicolo noleggiato) affinché la stessa potesse notificargli il verbale di contestazione di una violazione alle norme del codice della strada.

L'Autorità, alla luce degli elementi acquisiti, non ha ritenuto lecito il trattamento svolto posto che il riferimento della società di autonoleggio al codice della strada e ad obblighi contrattuali nei confronti della società proprietaria del veicolo non è risultato pertinente; inoltre, non è risultato acquisito il consenso dell'interessato a tale specifico trattamento, né è stata addotta dalla società l'esistenza di altro presupposto di liceità (artt. 23 e 24 del Codice).

È stato inoltre prescritto alla società di riformulare l'informativa da rendere alla clientela, atteso che quella prodotta agli atti non è risultata conforme all'art. 13 del Codice (*Provv.* 16 giugno 2010 [doc. *web* n. 1741982]).

Trattamento per finalità di *marketing* di dati personali contenuti nel Pubblico registro automobilistico

In numerosi quesiti e segnalazioni riguardanti l'utilizzabilità, da parte di operatori economici privati, dei dati personali contenuti nel Pubblico registro automobilistico (PRA) gli utenti lamentavano di aver ricevuto, da società private, alle quali non avevano mai comunicato il proprio recapito, comunicazioni pubblicitarie, offerte d'intervento per effettuare la revisione della propria vettura o questionari con finalità di ricerca statistica.

Con *provvedimento* 11 marzo 2010 [doc. *web* n. 1709295], in base al quadro normativo di riferimento (r.d.l. 15 marzo 1927, n. 436; r.d. 29 luglio 1927, n. 1814; l. 9 luglio 1990 n. 187; d.m. 514 del 1992), l'Autorità ha affermato che l'accesso al PRA delle società di *direct marketing* per acquisire dati a fini di invio di proposte commerciali non é risultato compatibile con gli scopi per i quali la normativa prevede la raccolta dei dati (art. 11, comma 1, lett. *b*), del Codice).

Il Pubblico registro automobilistico, infatti, è stato istituito (r.d.l. 15 marzo 1927) per assicurare un regime di pubblicità legale con riguardo al trasferimento della proprietà e ai

vincoli di privilegio costituiti sugli autoveicoli, nonché per fornire quelle informazioni sui veicoli che possono risultare utili a fini di "interesse pubblico".

Pertanto, per quanto pubblici (art. 24 del Codice), i dati contenuti nel PRA non possono essere utilizzati, in assenza di un preventivo consenso, per scopi unicamente commerciali o pubblicitari, essendo tali finalità incompatibili con il sistema di pubblicità legale cui il registro è preordinato e, al contempo, avulse da qualsiasi rilevante interesse sociale comunque richiesto dalla norma.

L'Autorità ha invece considerato legittimo l'utilizzo, anche senza consenso, dei dati personali contenuti nel PRA da parte delle società (o centri) di revisione e delle officine autorizzate, per inviare questionari o comunicazioni relativi all'imminente scadenza del periodo di revisione dell'auto.

Ha infatti ravvisato, in tali casi, la sussistenza di un rilevante interesse pubblico a far conoscere informazioni che contribuiscono a migliorare la sicurezza nella circolazione degli autoveicoli e a favorire la tutela ambientale.

Tale interpretazione risulta altresì suffragata dal fatto che l'ACI, in occasione della redazione del proprio regolamento per l'accesso ai dati del PRA (dapprima emanato ai sensi dell'art. 23, comma 4, del citato d.m. 2 ottobre 1992, n. 514 e successivamente modificato ed integrato il 19 giugno 2002, anche al dichiarato fine di adeguarne il contenuto alla l. n. 675/1996, *medio tempore* entrata in vigore) ha confermato che, tra le categorie di utenti che abbiano un rilevante interesse a conoscere i dati registrati nel PRA, vanno annoverate anche "le società del settore automobilistico", tra cui possono ricomprendersi anche i *cd.* "*centri di revisione*" (art. 3, lett. *d*), del predetto regolamento).

Autorizzazione al trattamento dei dati giudiziari da parte di società di revisione contabile

Sono state sottoposte all'esame dell'Autorità alcune richieste di autorizzazione al trattamento dei dati giudiziari relativi, in particolare, a clienti, soci e dirigenti di alcune società di revisione contabile. Tali richieste, tutte di analogo tenore, venivano giustificate dalle società istanti in base al quadro normativo statunitense (il *Sarbanes-Oxley Act* del 2002), che impone alle società di revisione contabile che svolgono prestazioni professionali in favore di società emittenti azioni o prodotti finanziari soggetti al controllo della *U.S. Securities and Exchange Commission* di comunicare al *Public Company Accounting*

Oversight Board –organismo istituito con finalità di monitoraggio, tra l'altro, delle medesime società di revisione– alcune informazioni concernenti eventuali procedimenti penali a carico dei soggetti sopra indicati, pena l'impossibilità di registrarsi presso lo stesso PCAOB e, conseguentemente, di svolgere la propria attività di revisione; tanto, muovendo dall'assunto, peraltro corretto, che non potesse trovare applicazione alla fattispecie in esame l'autorizzazione generale n. 7/2009.

L'Autorità, ha rigettato le istanze, poiché il trattamento di dati giudiziari oggetto delle richieste avrebbe determinato un conflitto tra la disciplina nazionale e comunitaria e la stessa normativa statunitense; tra l'altro lo stesso *Sarbanes-Oxley Act* prevede la possibilità di esentare le società non statunitensi dall'applicazione della normativa ivi contenuta, qualora il conferimento di determinate informazioni al *Public Company Accounting Oversight Board* nella procedura di registrazione possa violare una legge nazionale non statunitense (*provvedimenti* 3 giugno 2010 [doc. *web* nn. 1737838; 1737844; 1738372; 1737997; 1738015; 1738024; 1738030; 1738053]).

11.6. TRATTAMENTO DI DATI PER LA "TESSERA DEL TIFOSO"

Il Garante ha valutato la liceità di taluni trattamenti di dati personali svolti nella realizzazione del programma "tessera del tifoso" varato dall'Osservatorio nazionale sulle manifestazioni sportive-Dipartimento della pubblica sicurezza del Ministero dell'interno, a seguito di alcune istanze relative, in particolare a: l'assenza di un'idonea base giuridica in grado di giustificare l'obbligo di sottoscrizione della tessera; l'inidoneità dell'informativa presente sui moduli predisposti dalle società; l'inadeguatezza della stessa modulistica utilizzata per il rilascio della tessera; l'assenza di una "copertura" normativa relativamente al connesso trattamento di dati giudiziari; il rischio di profilazione degli utenti derivante dalle finalità di *marketing* connesse all'impiego della tessera; l'utilizzo di tecnologia *RFID* per scopi non chiaramente individuati, né previamente indicati all'utenza (*Provv.* 10 novembre 2010 [doc. *web* n. 1779725]).

All'esito dell'istruttoria il Garante ha ritenuto che, allo stato, non difetterebbero idonei presupposti normativi atti a giustificare il trattamento dei dati personali (anche giudiziari)

connesso all'adozione della tessera del tifoso, tenuto conto dell'inquadramento giuridico –eventualmente sindacabile in altra sede– già riconosciuto allo strumento dallo stesso Ministero dell'interno (secondo cui la tessera costituirebbe una "facilitazione" ai sensi dell'art. 8 del d.l. n. 8/2007). La mancata acquisizione, in sede di adesione al programma "tessera del tifoso", del consenso degli interessati relativamente alla gestione del rapporto in corso di instaurazione è risultata giustificata considerando il trattamento necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato (art. 24, comma 1, lett. *b*), del Codice). Sotto distinto profilo, non è risultato invece provato il rischio di localizzazione degli utenti in ragione del *chip* a tecnologia *RFID* presente sulla tessera, tenuto conto che quest'ultima è risultata leggibile dagli appositi dispositivi esclusivamente ad una distanza ravvicinata (non superiore ai 10 cm). Ciò, muovendo dall'ulteriore presupposto, di carattere più generale, che lo stesso trattamento correlato all'impiego di tecnologia *RFID* per finalità di accesso agli impianti sportivi è risultato necessario e non eccedente, attese anche le garanzie offerte sul piano della sicurezza e della velocizzazione degli accessi (avuto riguardo altresì all'elevato numero di spettatori presente, di solito, sugli spalti).

Per altro verso, il Garante ha invece riscontrato alcune "criticità" relativamente all'informativa resa agli interessati, all'acquisizione del loro consenso per finalità di *marketing*, alla qualificazione dei rapporti intercorrenti tra i soggetti coinvolti nell'iniziativa.

L'Autorità ha dunque prescritto alle società sportive coinvolte nel programma "tessera del tifoso" di integrare, ove necessario, l'informativa da rendere agli interessati e di predisporre moduli di adesione che consentano agli interessati di formalizzare anche il proprio diniego all'eventuale trattamento per finalità di *marketing*, anche da parte di società terze.

Le società sportive, inoltre, sono state invitate a valutare l'opportunità di predisporre moduli separati per ulteriori usi della tessera, per facilitare la comprensione delle caratteristiche e delle operazioni di trattamento effettuate dai soggetti coinvolti a vario titolo nell'iniziativa. Si è inoltre provveduto a richiamare l'attenzione delle società, ove interessate allo svolgimento di eventuali attività di profilazione, sulla necessità di acquisire un consenso specifico e distinto da parte degli interessati, nonché sulla necessità di provvedere alla notificazione del relativo trattamento (art. 37 del Codice).