8. Attività giornalistiche

8.1. Minori

Il Garante si è occupato nuovamente del delicato tema del rapporto tra libertà di informazione e tutela della riservatezza dei minori.

Vittime di abusi

L'Autorità è intervenuta d'urgenza con un *provvedimento* di blocco temporaneo del trattamento nei confronti di alcuni quotidiani che, nel riferire dell'avvio di un'indagine a carico di un personaggio di rilievo pubblico su presunti abusi sessuali ai danni della nipote minorenne, avevano diffuso dati ritenuti idonei a identificarla indirettamente (*Provv.* 25 giugno 2010). In particolare i quotidiani avevano indicato il legame parentale che legava la minorenne con l'indagato, individuato nominativamente, unitamente ad altre informazioni relative alla famiglia, nonché divulgato alcuni dettagli del referto stilato dai medici a seguito degli accertamenti sanitari compiuti sulla bambina. L'Autorità ha rilevato che, anche quando la vittima non viene individuata nominativamente, la diffusione di altre dettagliate informazioni che la riguardano può comunque renderla riconoscibile, in particolare nella cerchia delle relazioni sociali degli interessati e ciò costituisce una violazione del codice di procedura penale (art. 114, comma 6, c.p.p.), del codice di deontologia per l'attività giornalistica (art. 7) e della Carta di Treviso. Tale valutazione è stata confermata anche dopo il completamento dell'istruttoria e pertanto l'Autorità ha disposto nei confronti dei quotidiani interessati il definitivo divieto di ogni ulteriore diffusione di qualunque informazione idonea, anche indirettamente, a identificare la minore e a fornire dettagli del referto medico (*Provv.* 8 luglio 2010).

Analogo *provvedimento* di divieto è stato adottato nei confronti di un'emittente televisiva in relazione a una trasmissione nella quale è stata ospitata una ragazza ventunenne che ha affermato di essere stata vittima, quando era bambina, di ripetuti episodi di violenza sessuale da parte di uno zio. Nel corso della trasmissione, in risposta a una specifica domanda della conduttrice, la ragazza ha dichiarato che anche la sorella più piccola –ora quattordicenne e adottata– è stata vittima di episodi analoghi, e ha fornito alcuni elementi idonei a identificare indirettamente la sorella, in particolare il proprio cognome e il luogo

di svolgimento dei fatti di violenza. L'Autorità ha rilevato una violazione delle disposizione a tutela dei minori sopra richiamate (art. 114, comma 6, c.p.p.; art. 7 del codice di deontologia giornalistica; Carta di Treviso) le quali –ha ribadito– operano a maggior ragione con riferimento a minori vittime di violenze di natura sessuale. La stessa Autorità ha poi ritenuto irrilevante la circostanza che sia stata l'ospite della trasmissione a diffondere le notizie relative alla sorella in quanto, a prescindere dalla facoltà dell'ospite intervistato di raccontare liberamente la propria storia, incombe sul conduttore-intervistatore e sulla società emittente l'onere di rispettare le disposizioni di legge sopra richiamate impedendo che vengano diffuse, anche nel corso di interviste rilasciate da altri soggetti, informazioni idonee a identificare i minori. Nel caso di specie, tra l'altro, era emerso che la diffusione delle informazioni relative alla bambina era avvenuta su sollecitazione della conduttrice (*Provv.* 16 settembre 2010 [doc. *web* n. 1753383]).

Figli di personaggi noti

La *ratio* delle disposizioni a tutela dei minori consiste nel prevenire e/o eventualmente vietare un'informazione idonea a lederne la personalità e a comprometterne un armonico sviluppo. Come indicato nella Carta di Treviso, tale eventualità può non configurarsi se la notizia inquadra il minore in un contesto positivo. Tale principio, già ricordato dal Garante (cfr. *Relazione* 2009, pp. 126 e 127), ha ispirato la risposta a una segnalazione riguardante un servizio giornalistico con immagini che documentavano in termini positivi la dimensione familiare e affettiva di un noto esponente politico, dimensione a cui lo stesso esponente ha sempre dato autonomo risalto (cfr. anche art. 6 comma 2, del codice di deontologia cit.) (*Nota* 8 ottobre 2010). Analoghi princìpi hanno ispirato la risposta a una segnalazione relativa a un servizio giornalistico avente ad oggetto il nuovo film di un noto regista italiano ispirato al tema dei rapporti familiari, servizio contenente immagini che rappresentano il contesto delle relazioni familiari e affettive di alcuni dei protagonisti del film e che ritraggono la figlia minore dei segnalanti in quanto parte anch'essa del *cast* (*Nota* 26 aprile 2010).

Controversie familiari

In relazione a diverse segnalazioni riguardanti la trattazione, da parte degli organi di informazione, di vicende familiari che hanno portato all'allontanamento di un minore dai genitori e il suo affidamento ai servizi sociali, l'Autorità è stata chiamata a cogliere il punto

di equilibrio tra diritto di cronaca e di critica su provvedimenti giurisdizionali in materia di famiglia e il rispetto della sfera privata del minore, interessato da detti provvedimenti.

Il Garante, nel rispondere alle segnalazioni ha rilevato che non si può escludere in assoluto che provvedimenti in materia di rapporti familiari possano essere oggetto di cronaca e critica giornalistica.

Ciò premesso, la valutazione deve essere sempre fatta caso per caso. In uno dei casi esaminati, infatti, durante una trasmissione televisiva sono state riferite informazioni delicate (necessità di assunzione di psicofarmaci, asserite molestie sessuali) riconducibili a una minore identificata non solo indirettamente mediante la rivelazione dell'identità del padre intervistato, ma anche direttamente, attraverso la divulgazione del nome della stessa riproposto ripetutamente attraverso una didascalia in continuo scorrimento sul video durante l'intervista del padre. In questo caso l'Autorità ha ritenuto detto trattamento, nel suo insieme, non idoneo a soddisfare l'obiettivo di salvaguardia dell'interesse del minore sopra richiamato e ne ha dato comunicazione all'emittente televisiva interessata (*Nota* 15 ottobre 2010).

Adozioni

Il trattamento delle informazioni riguardanti vicende adottive presenta aspetti delicati anche quando coinvolge soggetti non più minori, trattandosi di informazioni che ricevono di per sé una particolare protezione da parte dell'ordinamento (l. 4 maggio 1983, n. 184 "*Disciplina dell'adozione e dell'affidamento dei minori*", modificata dalla l. 28 marzo 2001, n. 149).

L'Autorità è intervenuta nei confronti di una trasmissione televisiva che ha dedicato ripetutamente uno spazio alla narrazione di storie di adozione. In particolare, sulla base di alcune segnalazioni pervenute, il Garante ha ravvisato la necessità di disporre d'urgenza il blocco del trattamento dei dati trattati nel corso di alcune puntate in quanto ritenute in contrasto con la disciplina in materia di protezione dei dati personali e con la legge sull'adozione sopra citata (*Provv.* 8 aprile 2010 [doc. *web* n. 1718160].

Nelle more dell'istruttoria è stata riscontrata la violazione del *provvedimento* di blocco essendo stati trattati nuovamente dati personali attinenti alla vicenda adottiva raccontata nel corso di una delle puntate oggetto del blocco; l'Autorità ha quindi contestato all'emittente

televisiva la sanzione amministrativa di cui all'art. 162, comma 2-*ter* del Codice nonché segnalato il caso all'autorità giudiziaria per eventuali valutazioni di competenza (art. 170).

Inoltre, esaurita l'istruttoria, l'Autorità ha ribadito la propria valutazione in ordine all'illiceità di alcuni trattamenti.

Il Garante ha infatti rilevato che erano stati trattati dati personali relativi a vicende adottive, nonché diffusi dati idonei a identificare le predette persone, spesso associati a delicate informazioni sul loro passato. L'Autorità ha inoltre rilevato che gli appelli lanciati e le scritte apparse in sovraimpressione nel corso della trasmissione avevano evidenziato come il trattamento dei dati avesse come scopo la ricerca degli adottati da parte di membri della famiglia naturale di origine; ciò, in contrasto con la *ratio* della disciplina sulle adozioni la quale individua specificamente quali sono i presupposti perché l'adottato possa accedere a informazioni che riguardano la sua origine e l'identità dei genitori biologici, delineando un percorso preordinato a tutelare, attraverso particolari procedure e l'intervento dei soggetti e delle istituzioni competenti, la personalità dell'adottato –anche divenuto maggiorenne– e i contesti familiari interessati (artt. 27, 28, e 73, l. 4 maggio 1983, n. 184, modificata dalla l. 28 marzo 2001, n. 149). Alla luce di tali valutazioni, il Garante ha vietato l'ulteriore trattamento dei dati relativi alle vicende esaminate e ha, in termini generali, raccomandato all'emittente interessata di assicurare la dovuta osservanza delle disposizioni in materia di adozione (*Provv.* 6 maggio 2010 [doc. *web* n. 1718239]). Il *provvedimento* è stato impugnato dall'emittente ed è pendente giudizio dinanzi al giudice civile.

8.2. CRONACHE GIUDIZIARIE

L'Autorità ha risposto a diversi reclami e segnalazioni richiamando il principio, ormai consolidato, che la pubblicazione di dati personali relativi a procedimenti penali è ammessa anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 5, 6 e 12 del codice di deontologia). La valutazione deve essere fatta caso per caso, in prima battuta dal giornalista, nel quadro anche delle disposizioni che disciplinano il segreto delle indagini e il regime di pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.).

A seguito della diffusione su due siti Internet di un'ordinanza di custodia cautelare in carcere, pubblicata a corredo di una notizia concernente un presunto caso di corruzione, il destinatario della misura restrittiva si è rivolto al Garante lamentando un'illecita diffusione di dati "*di natura riservata e personale*", quali i numeri delle utenze cellulari oggetto di intercettazione, citati nel *provvedimento*. Compiuta l'istruttoria, il Garante ha accolto le richieste del segnalante, rilevando come la diffusione del *provvedimento* integrasse un trattamento a cui applicare la normativa *privacy* in materia di attività giornalistica.

Pertanto, pur riconoscendo il diritto alla manifestazione del pensiero da parte dell'associazione gestrice dei siti, che può esercitarsi anche mediante la pubblicazione di atti giudiziari non più coperti da segreto, il Garante ha ritenuto che la diffusione di dati quali i numeri di telefono, la residenza e i codici fiscali del segnalante e delle altre persone citate nel testo dell'ordinanza, avvenuta attraverso la pubblicazione in forma integrale del provvedimento giudiziario, abbia violato il principio dell'essenzialità dell'informazione, trattandosi di informazioni strettamente personali sicuramente sovrabbondanti e non indispensabili per rappresentare la vicenda giudiziaria.

Il Garante ha quindi vietato l'ulteriore diffusione disponendo la rimozione delle informazioni eccedenti dai due siti (*Provv.* 29 settembre 2010 [doc. *web* n. 1763096]).

Analoghe considerazioni sono state svolte in relazione alla pubblicazione delle utenze intercettate riportate nel documento inviato dalla Procura della Repubblica di Milano alla Giunta per le autorizzazioni a procedere della Camera dei deputati in relazione all'inchiesta che ha visto coinvolto, tra gli altri, il Presidente del Consiglio (*Nota* 20 gennaio 2011 e *Comunicato stampa* 21 gennaio 2011).

L'Autorità, anche in seguito a una segnalazione, ha avviato un'istruttoria in merito alla pubblicazione, anche su testate *online*, dell'audio degli interrogatori effettuati nell'ambito delle indagini sull'omicidio di una giovane donna di Avetrana. Tale circostanza è stata tempestivamente segnalata alla Procura della Repubblica che stava svolgendo le indagini la quale, come diffuso il 24 novembre 2010 dall'agenzia ANSA, ha provveduto al sequestro di detto materiale in relazione all'ipotesi di reato di "*pubblicazione arbitraria integrale di atti e documenti di un procedimento penale*".

Il richiamato parametro dell'essenzialità dell'informazione ha infine costituito la base nella valutazione di diversi trattamenti giornalistici che, pur se attinenti a fatti giudiziari di rilevante interesse pubblico, contenevano riferimenti a soggetti terzi i cui dati identificativi erano meritevoli di tutela –ad es., familiari, anche minorenni, di persone interessate da procedimenti penali (*Nota* 8 settembre 2010), parti lese (*Nota* 25 giugno 2010), ecc.– oppure a fatti pur relativi alle persone indagate ma estranei a quelli di indagine (ad es., il riferimento al ripetuto mancato superamento dell'esame d'avvocato da parte di un soggetto destinatario di un provvedimento di perquisizione (*Nota* 29 ottobre 2010).

Immagini di arresti

Il Garante è tornato ad occuparsi della pubblicazione delle fotografie che documentano operazioni di arresto e di quelle propriamente "segnaletiche".

Nel valutare alcune segnalazioni, il Garante ha ribadito il principio secondo il quale, di regola, è possibile pubblicare notizie relative a operazioni di arresto, salvo i limiti relativi alla diffusione di immagini che ritraggono persone in manette, di foto segnaletiche e di immagini comunque lesive della dignità della persona (art. 8 del codice di deontologia; cfr. anche *Relazione* 2007, par. 8.2.).

Ad avviso dell'Autorità, tali limiti sono stati superati in un caso nel quale è stata diffusa la foto segnaletica di una persona della quale sono stati oscurati solo gli occhi e di cui, sotto il riquadro della foto, sono state riportate le iniziali, rendendola di fatto riconoscibile. Uno dei quotidiani interessati dalla segnalazione aveva pubblicato anche le complete generalità della persona fotografata. Analoga valutazione è stata effettuata in un altro caso in cui, pur non essendovi elementi dai quali potesse desumersi, in base alle caratteristiche della foto, che si trattasse di una foto segnaletica, l'immagine pubblicata è apparsa lesiva della dignità della persona in quanto ritratta con la testa fasciata a seguito delle medicazioni ricevute. I predetti rilievi sono stati comunicati alle testate interessate, le quali si sono attivate per rimuovere le foto ancora presenti sulle edizioni *online* (*Note* 15 e 18 novembre 2010).

8.3. DATI SULLA SALUTE

Anche nel periodo di riferimento, come nel passato, si è reso necessario un richiamo al rispetto delle disposizioni che tutelano la riservatezza e la dignità di persone malate sia da

parte delle strutture sanitarie che forniscono informazioni sui loro pazienti sia da parte degli organi di informazione che accedono a tali informazioni (art. 83 del Codice; artt. 9, 10, 11 e 31 del codice di deontologia medica; art. 10 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; cfr. anche *Relazione* 2009, par. 8.4.).

Ciò è avvenuto per il caso di un giornale locale che aveva riferito sullo stato di salute di una persona ricoverata presso una struttura sanitaria, identificata con nome e cognome, descrivendo altresì la peculiare situazione in cui questa si era venuta a trovare (il fatto di essere stato "*dimenticato alla casa di riposo*" di cui "*nessuno pagava la retta*", le sue difficoltà di inserimento e di comunicazione all'interno della struttura, ecc.) (*Nota* 17 dicembre 2010).

Il Garante ha avuto altresì occasione di ricordare che la tutela della riservatezza e della dignità di una persona malata non viene meno neanche dopo il suo decesso (*Nota* 29 marzo 2010).

In seguito alla vicenda di un aborto farmacologico a Bari, il Garante ha invitato gli organi di informazione a tutelare l'anonimato e la riservatezza delle donne che effettuano interventi di interruzione della gravidanza (*Comunicato stampa* 8 aprile 2010).

8.4. ESPRESSIONE ARTISTICA E LETTERARIA

Nel periodo di riferimento diverse segnalazioni hanno prospettato una possibile illiceità del trattamento di dati personali, nell'ambito di pubblicazioni letterarie o comunque non giornalistiche in senso stretto (saggi, autobiografie, dizionari).

Nel fornire riscontro al riguardo, il Garante ha ricordato che l'art. 136, inserito nel Titolo XII della Parte II, del Codice ed intitolato "*Giornalismo ed espressione letteraria artistica*", estende l'applicazione delle disposizioni contenute nel Titolo stesso anche al trattamento "*temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale, di articoli, saggi e altre manifestazioni del pensiero*" (lett. *c*)) e che anche in relazione a tali trattamenti deve essere assicurato un bilanciamento tra la libertà di manifestare il proprio pensiero e il diritto alla riservatezza e alla protezione dei dati personali.

Pertanto –ha precisato il Garante– trovano applicazione le disposizioni che tutelano i minori e le informazioni sullo stato di salute; quelle che limitano la diffusione ai soli dati "*essenziali*" alla completezza dell'informazione e che danno rilievo alla particolare qualificazione dei personaggi citati nella narrazione (ad es., figure di rilevo pubblico) e, ancora, che consentono la pubblicazione delle informazioni già rese note dagli interessati (*Note* 11 giugno, 8 settembre, 14 dicembre 2010 e 5 gennaio 2011).

8.5. INFORMAZIONI RELATIVE A PERSONE E FATTI D'INTERESSE PUBBLICO

Nel 2010 sono pervenute segnalazioni e reclami relativi alla diffusione di dati personali concernenti personaggi pubblici o persone che esercitano pubbliche funzioni.

Il Garante ha ribadito il principio in base al quale vi sono margini più ampi nella diffusione di informazioni relative a tali persone, le quali possono riguardare, entro certi limiti, anche notizie attinenti alla vita privata.

L'Autorità tra l'altro, è intervenuto su un caso di diffusione di dati sanitari da parte di un quotidiano locale, che in un articolo aveva riportato, in fotografia, parte della cartella clinica del presidente di una regione e il referto di un altro esame sempre relativo al medesimo presidente.

Nel testo del *provvedimento*, si è rilevato che il servizio oggetto del reclamo riportava un fatto che può ragionevolmente considerarsi di rilievo pubblico, in quanto dava conto di una denuncia di presunta falsificazione della cartella clinica relativa al reclamante, presentata dal primario presso cui il reclamante aveva effettuato gli accertamenti clinici (denuncia che ha determinato l'apertura di un'indagine da parte della Procura della Repubblica).

In proposito, il Garante ha giudicato pertinente e non eccedente la diffusione della scheda di dimissione ospedaliera, ma non quella del referto, in quanto in quest'ultimo documento comparivano dettagli clinici ritenuti non essenziali. Il codice deontologico citato prevede, infatti, che "*la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita privata*" (art. 6) (*Provv.* 13 gennaio 2011 [doc. *web* n. 1787902]).

L'Autorità, inoltre, ha ricevuto alcune segnalazioni relative a servizi televisivi nell'ambito di due diverse puntate di un medesimo programma di informazione concernenti due noti personaggi esercitanti pubbliche funzioni. In entrambi i casi, il Garante ha sottolineato che tali servizi avevano ad oggetto fatti di interesse pubblico, con opinioni formulate in un contesto giornalistico nell'esercizio del diritto di cronaca e di critica, sicché non ha ritenuto necessario un suo intervento (*Note* 16 aprile 2010 e 17 gennaio 2011).

Il Garante si è pronunciato inoltre sulla diffusione su un quotidiano di una serie di *Sms* tra due personaggi che rivestono cariche pubbliche, ravvisando, nel caso di specie, l'interesse pubblico idoneo a giustificare tale diffusione (*Provv.* 3 febbraio 2011 [doc. *web* n. 1793828]).

8.6. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

Anche nel 2010 il Garante ha ricevuto diverse segnalazioni e ricorsi concernenti la libera disponibilità degli archivi storici *online*.

Giornali *online*

Al riguardo, è stato ribadito che la diffusione sul sito Internet di un quotidiano *online* di un articolo contenente informazioni su fatti anche molto delicati e piuttosto risalenti costituisce parte integrante dell'archivio storico della testata e non integra un illecito trattamento di dati personali. L'articolo, infatti, conteneva notizie relative a fatti veri e di interesse pubblico sia con riferimento al tempo della pubblicazione, sia attualmente, per eventuali ricerche sulla vicenda in questione.

Tuttavia, il Garante, tenendo conto delle peculiarità del funzionamento della rete, che può comportare la diffusione di un gran numero di dati personali riferiti a un medesimo interessato e relativi a vicende anche risalenti, e in considerazione del tempo trascorso, ha ritenuto che una perenne associazione all'interessato della vicenda stessa possa comportare un sacrificio sproporzionato dei suoi diritti.

L'Autorità, ha indicato pertanto, quale misura a tutela dei diritti dell'interessato, che la pagina *web* contenente i dati personali del ricorrente (quale è, anzitutto, il suo nominativo) sia sottratta alla diretta individualità all'atto della ricerca sui comuni motori di ricerca, pur restando tale pagina inalterata nel contesto dell'archivio e consultabile tele-

maticamente accedendo all'indirizzo *web* dell'editore (*Provv.* 22 luglio 2010 [doc. *web* n. 1748818]).

Invece, il Garante non ha accolto alcuni ricorsi volti ad ottenere l'aggiornamento delle notizie giudiziarie diffuse *online*, o comunque l'oscuramento dei dati del ricorrente o l'uso di iniziali in luogo del nome, in quanto ha rilevato che il trattamento, in origine effettuato per finalità giornalistiche, rientra ora, attraverso la conservazione nell'archivio *online* del quotidiano, tra i trattamenti effettuati per fini storici. Tale ulteriore finalità, per espressa previsione normativa (art. 99, comma 1, del Codice), è considerata compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati, rendendo pertanto lecito il perdurante trattamento (*Provv.* 18 febbraio 2010 [doc. *web* n. 1706475]; *Provv.* 15 luglio 2010 [doc. *web* n. 1746654]; *Provv.* 29 settembre 2010 [doc. *web* n. 1763552]).

Informazioni *online*

Sono continuate a pervenire segnalazioni nelle quali si chiede la cancellazione di dati e di immagini personali che risultano essere stati diffusi e in vario modo reperibili su Internet (ad es., sui comuni motori di ricerca, quale *Google*, su noti siti di condivisione di informazioni e video, quali *YouTube*, su *forum*, *blog*, o ancora su *social network* assai utilizzati e reputati lesivi della sfera personale dei segnalanti).

Con particolare riferimento a *forum* e *blog*, nei casi in cui sono stati ravvisati i presupposti, il Garante è intervenuto chiedendo ed ottenendo la cancellazione dei dati personali eccedenti all'amministratore o intestatario del *forum* o del *blog*, in qualità di contitolare del trattamento rispetto ai dati pubblicati dagli utenti ovvero ha chiesto la rimozione degli stessi all'*hosting provider* del sito, ai sensi dell'art. 16 del d.lgs. 70/2003.

Nei casi in cui, invece, è risultato che il titolare del sito Internet interessato non era stabilito nel nostro Paese, non è stato possibile applicare le tutele previste dal Codice (art. 5, comma 1).

In queste situazioni, al fine di fornire comunque una tutela all'interessato, il Garante, a fronte di una manifesta illiceità, ha contattato, sollecitando una collaborazione da parte dei *provider* stranieri, l'*hosting provider* del sito oggetto di segnalazione, richiedendo la rimozione dei contenuti lesivi, o, comunque ha fornito agli interessati l'indicazione del

soggetto titolare, estratto dai registri "*Whois*", a cui il segnalante potesse direttamente richiedere la rimozione immediata dei contenuti ritenuti illeciti in quanto diffamatori. Ciò, in ottemperanza a una prassi nota come "*notice and take down*", riconosciuta sia negli USA sia in ambito di Unione europea (cfr. Direttiva n. 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, recepita in Italia con il d.lgs. n. 70/2003) (*Note* 12 aprile e 28 luglio 2010).

9. Trattamento di dati personali attraverso Internet e tecnologie della comunicazione

9.1. Diffusione di dati sensibili su Internet

Il Garante è intervenuto con riguardo alla diffusione su siti *web* di informazioni anche di natura sensibile, in relazione alla pubblicazione *online* di un'intervista che richiamava i dati relativi alla salute di persone decedute.

Nell'inibire l'ulteriore diffusione di tali dati l'Autorità ha evidenziato come il riferimento allo stato di salute di una determinata persona, identificata o identificabile, da parte del giornalista, non possa prescindere dal rispetto della dignità, della riservatezza e del decoro personale della persona stessa e che tale tutela permane anche dopo la morte.

Il Garante ha poi evidenziato come il rispetto delle suddette garanzie possa essere invocato da chiunque abbia un interesse proprio ovvero agisca nell'interesse dell'interessato o per ragioni familiari meritevoli di protezione (*Provv.* 1° luglio 2010 [doc. *web* n. 1738303]).

9.2. *Forum* e *blog*

Il Garante si è occupato anche di segnalazioni presentate da persone fisiche o giuridiche riguardanti la diffusione su *forum* e *blog* di dati personali anche con riferimento a commenti sulla loro attività professionale o commerciale.

Ad esito dell'istruttoria condotta al riguardo di ciascuna, non si sono ravvisati i presupposti necessari per promuovere un *provvedimento* dell'Autorità.

Libera manifestazione del pensiero

L'Autorità, infatti, ha evidenziato che l'indicazione di alcuni dati personali (come la denominazione della società, il relativo indirizzo e la formulazione di commenti sulla sua attività e sui servizi resi dalla medesima) –sia a mezzo stampa, sia all'interno di un qualsivoglia sito *web*– costituisce una libera manifestazione del pensiero (*Nota* 4 febbraio 2011).

Ciò, anche quando i detti commenti sono contenuti, come talora è emerso, in una lettera inviata da un utente registrato a un determinato *forum* all'associazione che gestiva il medesimo. Tanto più quando la lettera in questione sia risultata rettificata, su istanza del segnalante interessato, nella parte che poteva apparire offensiva nei suoi confronti.

Ne consegue –come sottolineato dal Garante– che in tal caso la raccolta e la diffusione di dati personali pubblici, ad esempio nelle note relative al nome della società, così come nei commenti, possono avvenire anche senza il consenso dell'interessato, in quanto rientrano nell'ambito della manifestazione del pensiero.

L'Autorità ha comunque precisato che resta fermo il divieto di diffondere dati personali altrui ledendone la dignità o l'onorabilità (*Nota* 4 febbraio 2011).

È stato pertanto evidenziato che –in una considerazione necessariamente unitaria del nostro ordinamento giuridico– qualora il trattamento dei dati risulti illecito, per il mancato rispetto della normativa vigente (ad es., per eventuali profili diffamatori), è ovviamente possibile ricorrere alle forme di tutela previste dal codice civile e dal codice penale (risarcimento danni, querela, ecc.) da far valere dinanzi all'autorità giudiziaria.

Dati sanitari

I luoghi virtuali di comunicazione e circolazione dei dati, quali *social network*, *blog* e *forum* si sostituiscono sempre più ai luoghi fisici tradizionali, anche per la discussione su questioni di salute e quindi anche rispetto ai *cd.* "dati supersensibili".

Pazienti, specie se colpiti da malattie rare, usano Internet e *social network* per fornire e ottenere informazioni su medici, terapie e strutture specializzate.

Le "chiacchierate" fra utenti o i quesiti posti a medici *online* sugli esiti delle ultime analisi mediche o su una particolare malattia da cui si è affetti, pur evidentemente svolte in buona fede, rivelano però informazioni riservate che possono poi finire nella platea globale dei motori di ricerca.

Al riguardo, sono pervenute all'Ufficio alcune segnalazioni, in relazione alla reperibilità e diffusione, tramite il motore di ricerca *Google*, di dati sanitari inseriti dall'utente in determinati *forum* o *blog*.

In particolare, una ha riguardato la diffusione dello stato di malattia di un utente del sito *web* appartenente ad un'associazione dedita alla tutela di persone affette da una particolare patologia. Nell'ambito di un'istruttoria preliminare, l'Ufficio ha rivolto una richiesta di informazioni alla detta federazione, chiedendo altresì di indicare, se, e con quali modalità, gli utenti del predetto *forum* fossero idoneamente informati sulla circostanza che i dati personali da loro inseriti, compresi i dati sensibili oggetto di specifiche

discussioni all'interno del portale, fossero diffusi su Internet, nonché indicizzati da motori di ricerca esterni (*Nota* 28 maggio 2010).

Il titolare del sito *web* ha al riguardo evidenziato che il proprio *forum*, ai fini della registrazione, prevede semplicemente l'utilizzo di un *username* e di una e-mail, e non del nome e cognome, e che era stato l'utente, di sua iniziativa, a firmare tutti i suoi *post* nel *forum* ogni volta rivelando tali dati personali.

L'associazione, in ogni caso, che non aveva informato gli utenti del rischio di diffusione indiscriminata sul *web* dei dati inseriti né della possibilità di indicizzazione dei medesimi da parte dei motori di ricerca esterni, ha provveduto a eliminare dal *forum* ogni riferimento idoneo a identificare il segnalante ed a modificare l'informativa presente sul sito, includendo indicazioni anche sull'ambito di diffusione dei dati personali immessi degli utenti.

In un'altra segnalazione, un utente di un *forum* in materia di salute afferente ad una testata giornalistica *online*, ha rappresentato che, digitando il proprio numero di telefono sul motore di ricerca *Google*, si rinveniva una missiva da lui inviata, circa tre anni prima, ad un medico presente sul *forum* contenente vari suoi dati personali, anche di carattere sanitario (nome e cognome, età, provenienza geografica, malattia diagnosticata).

Al riguardo, l'Ufficio ha riscontrato che la pagina *web* contenente la lettera con i dati segnalati non era più rintracciabile (*Nota* 13 febbraio 2010); nel contempo, ha però rinvenuto un'altra pagina *web*, sulla quale era presente un ulteriore successivo *post* dello stesso segnalante nel medesimo *forum* riguardante il risultato dettagliato di un esame clinico, inserito *online* al fine di richiedere un consulto medico. Si precisa che nella medesima pagina *web* è risultata presente la risposta del medico allo specifico quesito, con indicazione della diagnosi da lui formulata, del livello di recidiva della malattia ipotizzata e della "*sorveglianza*" sanitaria periodica consigliata all'utente.

Alla luce di queste recenti segnalazioni, l'Autorità ha deciso di verificare, più in generale, il fenomeno dell'utilizzo e diffusione di dati sanitari nei *blog* e *forum*, considerando con metodo a campione, le impostazioni di accesso e utilizzo dei medesimi e il tipo di dati trattati da parte di utenti e gestori.

Questo analiticamente, con riferimento a *forum* e *blog* dedicati esclusivamente alla materia sanitaria o anche afferenti a testate giornalistiche *online*.

9.3. *FACEBOOK*

In misura superiore rispetto all'anno precedente, nel 2010 sono pervenute segnalazioni con le quali si è lamentato il trattamento illecito dei dati personali su *Facebook*.

L'Autorità, pur consapevole dei limiti territoriali dell'applicazione della normativa italiana, ha contattato il titolare del trattamento (*Facebook*) in un'ottica di collaborazione, sollevando alcune problematiche.

In particolare, l'Autorità ha chiesto informazioni relative all'avvenuta disattivazione di tre profili, lamentata dagli interessanti. Nel primo caso *Facebook* ha risposto elencando le ipotesi in cui provvede a disattivare i profili e ha sostenuto di non potere riattivare l'*account* del segnalante, non riuscendo a individuarlo (*Nota* 11 ottobre 2010). Nel secondo caso ha risposto che il segnalante aveva commesso una violazione delle condizioni contrattuali di *Facebook* (*Nota* 15 ottobre 2010). Nell'ultimo caso, invece, il profilo *Facebook* è stato riattivato (*Nota* 30 novembre 2010).

Inoltre, il Garante ha esaminato diverse segnalazioni con le quali alcuni utenti italiani non iscritti a *Facebook* hanno lamentato la ricezione di e-mail indesiderate da parte di questo *social network* (*Nota* 11 ottobre 2010).

In particolare, dagli accertamenti effettuati è risultato che *Facebook* mette a disposizione degli utenti iscritti la possibilità di usare uno strumento, denominato "*friend-finder*", attraverso il quale –in modo automatico– questi possono inserire tutti i contatti presenti nella propria casella di posta elettronica o nelle rubriche appartenenti ad altri servizi di messaggistica istantanea. A seguito di questo inserimento, *Facebook* provvede ad inviare a questi indirizzi e-mail messaggi di invito per l'iscrizione al *social network*, elaborando, automaticamente, un unico elenco, contenente tutti i nominativi degli utenti già iscritti al *social network* e che hanno inserito un medesimo indirizzo di posta elettronica. Pertanto, i contatti suggeriti agli utenti non iscritti, mediante l'e-mail inviata a costoro da *Facebook*, corrispondono a tali persone, già iscritte al *social network*,

che hanno inserito l'indirizzo di posta elettronica dell'utente non iscritto nei *database* di *Facebook*.

Periodicamente, il *social network* invia una nuova e-mail per ricordare di iscriversi, aggiornando anche l'elenco dei "*potenziali amici*" individuati da *Facebook*.

Il Garante ha rilevato che si verifica in tal modo non soltanto un'attività di *spam* da parte del *social network*, ma anche un'attività di profilazione dell'utente non iscritto, cui sono infatti associati periodicamente una serie di "*potenziali amici*" tra gli utenti della piattaforma.

A seguito di queste segnalazioni, inoltre, il Garante ha interpellato tutte le autorità europee, allo scopo di conoscere se avessero ricevuto analoghe segnalazioni. È emerso che il profilo in questione è stato affrontato soltanto dall'autorità tedesca.

Il Garante ha, poi, rigettato un ricorso nel quale una persona iscritta a *Facebook* aveva lamentato di essere stata "*taggata*" da un'altra, in particolare mediante una foto utilizzata per una campagna di sensibilizzazione sul tema dell'*AIDS* e dell'omosessualità, così svelando l'orientamento sessuale di tutti i soggetti "*taggati*", compreso il proprio. Il Garante ha osservato che, poiché la pagina *web* in cui risultava la segnalante non era stata oggetto di diffusione o di comunicazione sistematica, tale utilizzo della foto doveva considerarsi effettuato per fini esclusivamente personali (art. 5, comma 3, del Codice) e non era pertanto soggetto all'applicazione delle norme del Codice (*Provv.* 18 febbraio 2010 [doc. *web* n. 1712776]).

L'Ufficio è intervenuto anche riguardo alla segnalazione di un lavoratore licenziato dalla propria società a causa dell'utilizzo che il medesimo aveva fatto di *Facebook*.

In particolare, il lavoratore aveva lamentato l'utilizzo da parte della società di alcune fotografie (scattate sul luogo di lavoro e sul cui sfondo erano visibili disegni –a detta dell'azienda– coperti da segreto industriale) tratte dal proprio profilo *Facebook*.

Il segnalante aveva affermato la illiceità del trattamento dei dati in questione, sulla base del carattere "*chiuso*" del suo profilo, riservato a una cerchia ristretta di utenti, tra i quali non rientrava il datore di lavoro, e dell'assenza del consenso dell'interessato *ex* art. 23 del Codice.

Dall'istruttoria, è emersa invece la possibilità per il datore di lavoro di utilizzare lecitamente le foto in questione, in quanto la consultazione era consentita non solo ai contatti scelti dal dipendente (i cd. "*amici*"), ma a una comunità più vasta, i *cd.* "*amici degli amici*", cioè ai contatti scelti dagli amici dell'interessato, quindi a una cerchia di utenti sostanzialmente indeterminabile (*Nota* 26 agosto 2010).

9.4. INFORMATIVA E CONSENSO NELLA COMPILAZIONE DI *FORM* DI REGISTRAZIONE *ONLINE*

L'attività di verifica dell'Autorità e le lamentele di numerosi utenti del *web* sulla legittimità dei trattamenti di dati personali richiesti in occasione della compilazione di *form online* hanno portato, anche per l'anno di riferimento, all'adozione di diversi provvedimenti di carattere inibitorio e prescrittivo.

È stato rilevato su istruttorie avviate a seguito di segnalazioni che in alcuni casi sono state utilizzate modulistiche alquanto ingannevoli. Le segnalazioni sono state presentate da utenti che, dopo essersi iscritti ad alcuni servizi sul *web*, sono stati destinatari di attività di *spamming*. In taluni casi è stato rilevato infatti che, nella compilazione della modulistica per la registrazione a servizi *online*, al trattamento da parte di terzi dei propri dati personali il consenso a ricevere pubblicità veniva inserito quale necessario presupposto per la prestazione richiesta.

In altri casi è risultato che con un unico consenso veniva indicata sia la finalità di *marketing*, sia l'attività di profilazione, nonché la comunicazione dei dati personali a terzi e l'utilizzo di strumenti automatizzati (fax, e-mail, *Sms*, telefonate preregistrate per fini promozionali).

Come già ribadito nei provvedimenti adottati anche nell'anno 2009, i titolari del trattamento non devono richiedere il consenso per i trattamenti effettuati per eseguire obbligazioni derivanti da contratti di cui è parte l'interessato.

Con riferimento invece agli ulteriori trattamenti, quali l'attività di promozione tramite telefono o posta cartacea, di profilazione, di comunicazione di dati a terzi o di attività pubblicitaria eseguita con gli strumenti automatizzati di cui all'art. 130, "*il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato*" (art. 23, comma 3, del Codice).

Si è quindi riscontrata la illegittimità della modulistica nella quale veniva raccolto un consenso non specifico per le diverse finalità.

Per quanto riguarda l'informativa, nel caso in cui è prevista la cessione dei propri dati personali a soggetti terzi che non rivestono la qualità di responsabili del trattamento, è necessario, non solo richiedere uno specifico e libero consenso all'interessato, ma anche che questi sia reso edotto, mediante idonea informativa, almeno della categoria di soggetti cui sono trasmessi i suoi dati (art. 13 del Codice, in particolare, comma 1, lett *d*)). Un'altra anomalia riscontrata in diverse informative rilasciate *online*, ha riguardato la non menzionata possibilità riconosciuta agli interessati di poter revocare il consenso prestato e, soprattutto, di potersi opporre in qualsiasi momento al trattamento effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale. Tali finalità devono essere distintamente indicate nell'informativa e devono essere oggetto di altrettanti distinti consensi (cfr. art. 7, comma 4, del Codice).

Alla luce di quanto sinora evidenziato, l'Autorità, come detto, ha adottato nel corso dell'anno 2010, diversi provvedimenti dei quali i più rappresentativi sono di seguito richiamati.

In particolare, alla società E-Dreams S.r.l., specializzata nella prenotazione *online* di voli, hotel e pacchetti turistici è stato vietato l'ulteriore trattamento dei dati illegittimamente acquisiti e prescritto di riformulare il modulo di registrazione al sito, con l'obbligo di garantire ai clienti la possibilità di prestare consensi differenziati (*Provv.* 8 aprile 2010 [doc. *web* n. 1721205]).

È stato poi vietato, ad una società che gestisce i siti *web* di quattro emittenti radiofoniche a livello nazionale del Gruppo Finelco S.p.A., il trattamento dei dati personali degli ascoltatori raccolti in modo non conforme alla normativa vigente. A questa società è stato altresì prescritto di riformulare i moduli di registrazione con l'obbligo di garantire agli utenti la possibilità di prestare consensi differenziati, nonché di modificare l'informativa, indicando chiaramente le categorie di soggetti cui possono essere comunicati i dati (*Provv.* 22 luglio 2010 [doc. *web* n. 1741988]).

Come detto, l'Autorità ha riscontrato casi in cui i segnalanti sono stati destinatari di attività di *spamming* tramite e-mail da parte di alcune società, le quali, secondo gli esiti delle istruttorie condotte dall'Autorità, avevano acquisito gli indirizzi dal sito *web* della Fiera di Milano, gestito dalla società Expopage S.p.A, dove le dette società si erano registrate in occasione di una manifestazione fieristica.

Nella fattispecie, il *form* di registrazione al sito richiedeva un unico consenso all'utilizzo dei dati degli interessati da parte dell'ente organizzatore, e anche di terzi, aziende e/o società che svolgevano attività e perseguivano varie finalità, fra cui quella promozionale e quella di *marketing*.

Anche nei confronti di Expopage S.p.A., pertanto, è stato emanato un *provvedimento* di carattere inibitorio e prescrittivo rispetto alla modifica della formula per l'acquisizione del consenso distinta per ciascun tipo di trattamento (*Provv.* 7 ottobre 2010 [doc. *web* n. 1763037]).

Da ultimo, si segnala l'intervento compiuto nei confronti di un noto sito Internet (*www.casa.it*) destinato alla ricerca, sull'intero territorio nazionale, di immobili a vario fine (locazione, vendita, acquisto, ecc.).

Anche in tal caso, nel *form* di registrazione veniva richiesto un unico consenso, peraltro configurato come preimpostato, per diverse finalità e non veniva chiaramente indicata nell'informativa la categoria di soggetti cui sarebbero stati trasmessi i dati degli iscritti (*Provv.* 15 luglio 2010 [doc. *web* n. 1741998]).

9.5. *GOOGLE STREET VIEW*: LA TUTELA DEI "*PAYLOAD DATA*", L'UTILIZZO DELLE *GOOGLE CAR* E L'OBBLIGO INFORMATIVO

L'Autorità quest'anno ha avviato un approfondimento sul servizio *Street View* reso dalla società statunitense *Google*, all'esito della quale ha adottato per la prima volta nei suoi confronti due provvedimenti, inibitori e prescrittivi.

In particolare, con il *provvedimento* 9 settembre 2010 [doc. *web* n. 1750529], il Garante ha imposto a *Google*, il quale aveva raccolto sia dati relativi alla presenza di reti *Wi Fi* (*Wireless Fidelity*) sia frammenti di comunicazioni elettroniche trasmesse dagli utenti

su alcune reti *Wi Fi* non protette da protocolli sicuri e da cifratura (*cd.* "*payload data*"), di bloccare qualsiasi trattamento dei suddetti *payload data* captati dalle *Google car* (veicoli che circolano nelle città acquisendo immagini fotografiche di luoghi e persone poi pubblicate *online* ai fini del servizio *Street View*) e ha inviato gli atti all'autorità giudiziaria per la valutazione dell'eventuale rilevanza penale.

Nel corso del procedimento, avviato nel mese di maggio, *Google* ha verificato che la raccolta dei dati era avvenuta erroneamente e che le informazioni raccolte erano talmente frammentate da non poter essere considerate dati personali. La società ha inoltre dichiarato che i menzionati dati sarebbero stati conservati su *server* negli Stati Uniti e mai utilizzati, né comunicati a terzi.

Ad avviso dell'Autorità, invece, una tale raccolta di informazioni, essendo stata effettuata in modo sistematico e per un considerevole periodo di tempo (aprile 2008 - maggio 2010), ha comportato la concreta possibilità che alcune delle informazioni "*catturate*" abbiano natura di dati personali e che quindi possano consentire di risalire a persone identificate o identificabili.

Google, pertanto, potrebbe aver violato non solo il Codice, ma anche alcune norme del codice penale, come quelle che puniscono le intercettazioni fraudolente di comunicazioni effettuate su un sistema informatico o telematico (art. 617-*quater*) e l'installazione, fuori dai casi consentiti dalla legge, di "*apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico*" (art. 617-*quinquies*).

Considerato inoltre che i "*payload data*" possono costituire elementi di prova delle eventuali violazioni destinate alla valutazione della magistratura, il Garante ha ritenuto che essi non debbano essere cancellati dai *server* nei quali sono conservati e ne ha disposto il blocco, imponendo a *Google* di sospendere qualunque trattamento.

Sempre in relazione al servizio *Street View*, l'Autorità è intervenuta anche successivamente, con il *provvedimento* 15 ottobre 2010 [doc. *web* n. 1759972], con il quale ha prescritto a *Google* di informare i cittadini italiani della presenza delle *Google car*, chiedendo alla società statunitense di fornire ai cittadini dettagliate notizie sul passaggio delle auto,

affinché possano decidere in piena libertà i propri comportamenti ed eventualmente scegliere di sottrarsi alla "*cattura*" delle immagini e allontanarsi dai luoghi ripresi.

Il Garante ha tenuto conto di numerose segnalazioni pervenute all'Autorità da cittadini che non desideravano comparire sulle fotografie pubblicate *online* e ha ritenuto, in via del tutto innovativa rispetto al passato, che al trattamento di dati effettuato dal servizio *Street View* si debbano applicare le norme del Codice, essendo tale servizio effettuato con strumenti (vetture, impianti fotografici, ecc.) situati nel territorio italiano.

Nello specifico, le *Google car* dovranno essere facilmente individuabili, attraverso cartelli o adesivi ben visibili, che indichino in modo inequivocabile che si stanno acquisendo immagini fotografiche per il servizio *Street View*.

Alla società californiana è stato ordinato inoltre di pubblicare sul proprio sito *web*, tre giorni prima che inizino le riprese, le località visitate dalle vetture in questione.

Per le grandi città è necessario indicare i quartieri in cui circoleranno le vetture. Analogo avviso deve essere pubblicato da *Google* sulle pagine di cronaca locale di almeno due quotidiani e diffuso per mezzo di un'emittente radiofonica locale per ogni regione visitata.

Infine, alla società californiana è stato anche imposto di nominare un proprio rappresentante sul territorio italiano al quale possano rivolgersi i cittadini per la tutela dei loro diritti, con particolare riferimento a quelli di cui all'art. 7 ss. del Codice.

9.6. DATI PERSONALI UTILIZZATI A FINI DI PROFILAZIONE E *MARKETING*

Profilazione della clientela da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico

Nel 2010 è proseguita l'attività di verifica preliminare relativa al corretto utilizzo dei dati personali aggregati dei clienti per finalità di profilazione da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, sulla base del *provvedimento* generale del 25 giugno 2009 [doc. *web* n. 1629107], che aveva stabilito i parametri e le misure minime da seguire.

In tal senso l'Autorità ha emanato una serie di provvedimenti a seguito delle diverse istanze di *prior checking* inviate dai gestori di telefonia presenti sul mercato e ha contestualmente avviato l'attività ispettiva relativamente alla verifica del corretto adempimento delle misure tecnico-giuridiche prescritte.

Il Garante ha concluso le attività di carattere ispettivo e di accertamento relative al trattamento di dati personali contenuti in banche dati utilizzate per finalità di *marketing* iniziate nel 2008 (cfr. *Relazione* 2008, p. 112; *Relazione* 2009, p. 142).

Al termine delle ispezioni sono stati aperti dieci procedimenti amministrativi nei confronti dei soggetti ispezionati: Addressvitt S.r.l., Ammiro partners S.r.l., Cemit Interactive Media S.p.A., Consodata S.p.A., Edipro S.a.s., Fast*web* S.p.A., Opitel S.p.A., Postel S.p.A., Sky Italia S.r.l., Telextra S.r.l.

Nell'ambito di ciascun procedimento sono stati adottati, dopo quelli del 2009, altri provvedimenti inibitori e/o prescrittivi per violazioni al Codice. In particolare, il quadro complessivo ha evidenziato il persistere di un utilizzo di dati personali raccolti in violazione del Codice e l'adozione di procedure elusive della normativa.

È risultato infatti che la maggior parte delle società non forniva alcuna informativa, sia quando raccoglieva i dati direttamente presso gli interessati (ad es., attraverso moduli o *coupon*) sia, più frequentemente, quando li raccoglieva presso terzi. Le stesse società, inoltre, non avevano richiesto o non erano in grado di documentare un consenso al trattamento dei dati per le finalità di *marketing* o, nell'ipotesi di cessione del *database*, per la comunicazioni dei dati medesimi a terzi.

Per la prima volta, infine, relativamente ad alcune sanzioni amministrative, è stata applicata la sanzione prevista dall'art. 164-*bis*, comma 2 (banche dati di rilevanti dimensioni o interesse) e l'aggravante del successivo comma 3 (in relazione all'elevato numero di interessati). I relativi procedimenti sanzionatori sono ancora in corso (v., più nel dettaglio, par. 19.4.2.).

Come è noto, la disciplina del *marketing*, limitatamente a quello effettuato mediante l'utilizzo del telefono, è stata recentemente modificata dal legislatore; tuttavia si rileva che il nuovo quadro normativo ha disposto una modifica sostanziale alla materia valida *pro futuro* e pertanto ha avuto un impatto limitato sugli esiti dei procedimenti amministrativi relativi alle citate società, prima dell'entrata in vigore delle novità normative.

Raccolta del consenso per diverse finalità e modalità del trattamento

In questo ambito è emersa la necessità di fornire alcuni chiarimenti in merito al requisito del consenso di cui all'art. 23 del Codice. A fronte di un'interpretazione della norma che comporterebbe la non equivalenza tra specificità e necessaria modularità del con-

senso, con la conseguente possibilità di acquisire dall'interessato un consenso indifferenziato per i diversi trattamenti effettuati dal titolare, il Garante ha ribadito il proprio costante orientamento secondo cui il consenso deve invece essere inteso come specifico per ogni finalità del trattamento, anche nel rispetto dei princìpi sanciti dall'art. 11 del Codice. Ciò con la conseguenza di dover necessariamente distinguere le finalità di *marketing* da quelle di profilazione, essendo illecito un consenso mirato ad autorizzare, con un'unica formulazione, una pluralità di trattamenti ben distinti (*Note* 26 marzo 2010 e 23 dicembre 2010).

Anche con riguardo all'interpretazione dell'art. 130 del Codice, ed in particolare del comma 2, l'Autorità nelle note suindicate, ha avuto modo di chiarire la propria posizione. La norma infatti non può essere intesa, come pure proposto, nel senso di ritenere legittimo il trattamento dei dati attraverso il riscorso a modalità automatizzate (ad es., *Sms*, *Mms*, posta elettronica e telefax) anche se all'utente non sia stato richiesto uno specifico consenso, dovendosi, al contrario, ritenere necessaria l'acquisizione di un consenso *ad hoc* posta la peculiarità del mezzo comunicativo utilizzato.

Il Registro delle opposizioni

In concomitanza con l'entrata in funzione del Registro pubblico delle opposizioni, introdotto dalla recente riforma della disciplina normativa del *telemarketing* (v., più nel dettaglio, par. 1.1.), il Garante ha adottato un *provvedimento* generale (19 gennaio 2011 [doc. *web* n. 1784528], in *G.U.* 31 gennaio 2011, n. 24) rivolto a tutti gli operatori che intendano utilizzare i dati personali presenti negli elenchi telefonici per attività di *telemarketing* e, più precisamente, per effettuare chiamate con operatore ai fini di invio di materiale pubblicitario, vendita diretta, ricerche o comunicazioni commerciali.

Come prescrive il disposto del nuovo art. 130 del Codice, dall'entrata in vigore della nuova disciplina gli operatori non possono più contattare telefonicamente coloro che, presenti in elenchi telefonici, abbiano iscritto la propria numerazione nel Registro. Il Garante, con il citato *provvedimento*, ha chiarito alcune ipotesi che potevano risultare dubbie, stabilendo *in primis* che la riforma legislativa (*cd.* "*opt out*") si applica ai dati di coloro che sono presenti in qualunque elenco telefonico, comprendendo, quindi, anche i dati presenti negli elenchi *cd.* "*categorici*".

Ha stabilito inoltre che qualora un interessato si sia opposto al trattamento dei suoi dati personali nei confronti di uno specifico titolare in epoca precedente all'entrata in vigore del Registro, egli non può essere chiamato in ogni caso da quel titolare, a prescindere dall'iscrizione nel Registro. Analogamente, se l'interessato ha manifestato un consenso specifico a ricevere telefonate promozionali nei confronti di un titolare determinato, quest'ultimo potrà continuare a contattarlo, anche se la numerazione risulterà iscritta nel Registro, sempreché sia in grado di documentare per iscritto tale consenso, come dispone l'art. 23 del Codice.

L'Autorità ha altresì chiarito che con l'entrata in funzione del Registro vengono meno le deroghe introdotte negli anni in tale materia dal Garante e pertanto non possono più essere utilizzate le numerazioni telefoniche contenute in banche dati comunque formate (comprese quelle costituite utilizzando i dati estratti dagli elenchi telefonici prima del 1° agosto 2005), senza aver prima acquisito uno specifico consenso.

Infine, il Garante ha stabilito che, per quanto riguarda le numerazioni presenti in pubblici registri, elenchi, atti o documenti conoscibili da chiunque esse potranno essere utilizzate solo se le telefonate promozionali risultino direttamente funzionali all'attività svolta dall'interessato (sempre che questi non si sia opposto) o se il *telemarketing* sia previsto dalla normativa di riferimento.

Modelli di informativa resa agli abbonati dagli operatori telefonici

Il Garante con *provvedimento* 24 febbraio 2011 [doc. *web* n. 1794638] ha definito i nuovi modelli di informativa e di richiesta di consenso che le società telefoniche devono utilizzare per informare i nuovi e i vecchi abbonati sulle nuove modalità da utilizzare per non ricevere telefonate pubblicitarie.

Nei due modelli vengono specificati i cinque modi per potersi iscrivere al Registro (per posta, tramite numero verde, via e-mail, via fax, direttamente sul sito *web* della Fondazione Bordoni).

Il primo modello riguarda i nuovi abbonati alla telefonia, fissa e mobile, e coloro che cambiano operatore richiedendo la cosiddetta "portabilità del numero". Il modulo dovrà essere fornito al momento della stipula del contratto, oltre che inserito nei siti *web* degli operatori telefonici. Consentirà, anche di decidere se comparire negli elenchi telefonici ed

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).