

8. ATTIVITÀ GIORNALISTICA E TECNOLOGIE DELLA COMUNICAZIONE

8.1. MINORI

Vittime di abusi

L'Autorità è intervenuta in diverse occasioni nei confronti di testate giornalistiche che, occupandosi di episodi di violenza sessuale su minori, hanno violato le specifiche garanzie poste a tutela di tali soggetti. In particolare, con riferimento a tre diversi casi di cronaca, il Garante ha riscontrato che alcuni giornali, pur omettendo nome e cognome delle vittime, avevano riportato numerosi dettagli riferibili alle vittime stesse (*ad es.*, iniziali del nome e cognome, sesso, età) e al contesto familiare e sociale di vita (*ad es.*, quartiere di residenza, tipologia di scuola frequentata, professione dei genitori e di parenti, presenza in famiglia di fratelli o sorelle e/o di animali domestici, luoghi di villeggiatura frequentati, *ecc.*) o, ancora, dati relativi all'autore della violenza (*ad es.*, grado di parentela con la vittima, professione, stato civile *ecc.*), la cui compresenza nel servizio giornalistico (diversamente articolata nei tre casi esaminati), ad avviso dell'Autorità, era idonea a rendere identificabili le vittime stesse. Nei riguardi delle testate interessate il Garante ha, dunque, disposto un divieto del trattamento per la violazione del principio di “*essenzialità dell'informazione*” (art. 137, comma 3, del Codice) e delle specifiche disposizioni a tutela dei minori. Infatti – fermo restando il divieto di carattere generale previsto dall'art. 734-*bis* c.p., di divulgare le generalità e l'immagine della persona offesa da atti di violenza sessuale, nel caso in cui la persona offesa da un reato sia minore di età – l'ordinamento vieta la divulgazione di elementi che anche indirettamente possano portare alla sua identificazione (art.114, comma 6, c.p.p.; art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso) (*Prov. 10 luglio 2008* [doc. *web* n. 1536583]; *Prov. 2 ottobre 2008* [doc. *web* n. 1557470]; *Prov. 16 febbraio 2009* [doc. *web* n. 1590076]).

Al di fuori di episodi di cronaca così gravi, per altri tipi di notizie segnalate al Garante e coinvolgenti minori (episodi di bullismo nelle scuole, casi di risultati scolastici oggetto di vertenze giudiziarie,) l'Ufficio, pur non ravvisando i presupposti per promuovere l'adozione di un *provvedimento* di divieto, ha ritenuto comunque opportuno richiamare l'at-

tenzione delle testate interessate dalle segnalazioni sul principio, espressamente enunciato dal codice di deontologia, in base al quale il diritto del minore alla riservatezza deve sempre essere considerato come primario rispetto al diritto di critica e di cronaca (art. 7 *cit.*).

Al Garante è stato chiesto di esprimersi in merito alla diffusione di un servizio televisivo girato presso alcuni campi nomadi di Roma. L'Autorità ha osservato che, con riferimento alla scelta di riprendere scene collettive di minori, ancorché riconoscibili, la diffusione delle immagini poteva ritenersi giustificata dal principio di “*essenzialità dell'informazione riguardo a fatti di interesse pubblico*”, anche alla luce della rilevante finalità di denuncia riguardo alle condizioni di disagio in cui tali minori si trovavano a crescere. Diversa, invece, è stata la valutazione per una specifica fase della trasmissione nella quale un minore riconoscibile è stato direttamente coinvolto in un'intervista su argomenti particolarmente delicati; ciò è apparso in contrasto con le indicazioni contenute al riguardo dalla Carta di Treviso richiamata espressamente dall'art. 7 del codice di deontologia.

8.2. CRONACHE GIUDIZIARIE

Anche nell'anno di riferimento sono stati esaminati numerosi casi relativi alle cronache giudiziarie.

In particolare, sono pervenute segnalazioni concernenti la pubblicazione di dati e immagini relativi alle vittime di reato, nelle quali l'Autorità ha chiarito che il limite dell'“*essenzialità dell'informazione*” va valutato con particolare rigore quando il trattamento riguardi dati personali di persone che sono state vittime di episodi criminosi. Tale rigore si giustifica anche alla luce di una specifica considerazione degli ulteriori rischi cui la diffusione di tali dati può esporre l'interessato, tanto più considerato il contesto sociale o familiare in cui egli è già inserito. In tale ambito sono stati adottati dal Collegio due provvedimenti di divieto di ulteriore diffusione nei confronti di quotidiani che avevano riportato dati eccedenti rispetto alla finalità di informazione sui reati in questione: il primo, perché aveva diffuso riferimenti idonei a identificare in modo diretto la persona offesa del reato di “*circonvenzione di incapace*”, unitamente a delicati riferimenti attinenti alle sue condizioni psichiche (*Prov. 5 giugno 2008 [doc. web n. 1527037]*); il secondo,

in quanto aveva diffuso riferimenti idonei a identificare una donna vittima di aggressione e di violenza sessuale da parte del coniuge (*Prov. 13 ottobre 2008 [doc. web n. 1563958]*).

L'Ufficio ha altresì esaminato e dato riscontro a segnalazioni e reclami riguardanti la pubblicazione di dati personali di persone sottoposte a misure cautelari, a indagini o a condanna. L'Autorità ribadendo principi ormai consolidati, ha chiarito che la pubblicazione dei dati relativi a procedimenti penali è ammessa anche senza il consenso dell'interessato, ma nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 5, 6 e 12 del menzionato codice di deontologia), da valutarsi in concreto, caso per caso, e nel rispetto delle disposizioni che tutelano il segreto delle indagini e degli atti processuali (artt. 114 e 329 c.p.p.). Si segnala, in questo ambito, il reclamo presentato da un noto personaggio, che lamentava la diffusione di dati relativi a un accertamento da parte dell'Agenzia delle entrate per evasione fiscale. Nella risposta dell'Ufficio sono stati richiamati i principi dell'esercizio del diritto/dovere di informazione e quello di trasparenza dell'attività giudiziaria, in base ai quali i dati relativi a persone oggetto di indagine, di regola, possono essere pubblicati, venendo in rilievo l'interesse pubblico a conoscere i fatti ivi descritti.

Tali principi sono stati nuovamente ricordati dal Garante in relazione altresì alla pubblicazione di intercettazioni di conversazioni telefoniche o di altro materiale di indagine, rappresentando a tutti i *media* la necessità di valutare con il massimo scrupolo e con senso di responsabilità la sussistenza dell'interesse pubblico alla eventuale diffusione delle informazioni e raccomandando il più rigoroso rispetto delle leggi in vigore, del codice deontologico e dei principi posti a tutela della persona (*Comunicato stampa 2 luglio 2008*). In più occasioni è stato lamentato il contenuto diffamatorio di alcune notizie pubblicate. In proposito l'Ufficio ha ricordato che, per questo specifico profilo, non possono essere invocate disposizioni in materia di protezione dei dati personali, bensì altre specifiche forme di tutela (rettifica, risarcimento dei danni, querela) previste dal codice civile, dal codice penale e dalla legge sulla stampa (l. 8 febbraio 1948, n. 47), da far eventualmente valere dinanzi al giudice ordinario.

8.3. TUTELA DELLA DIGNITÀ DELLA PERSONA E DIFFUSIONE DI INFORMAZIONI RELATIVE ALLE ABITUDINI SESSUALI

Il Garante si è occupato della cronaca relativa all'omicidio della studentessa inglese avvenuto a Perugia il 2 novembre 2007.

Già nel corso del 2008 l'Autorità era intervenuta nei confronti di un'emittente televisiva che aveva diffuso alcune immagini del corpo della giovane raccolte dalla Polizia scientifica durante uno dei sopralluoghi sul luogo dell'omicidio. Il Garante ha ritenuto che la diffusione delle predette immagini non fosse giustificata dal punto di vista dell'“*essenzialità dell'informazione riguardo a fatti di interesse pubblico*” e fosse gravemente lesiva della dignità della persona e ne ha, pertanto, vietata l'ulteriore diffusione.

Il Garante ha poi ricevuto un reclamo sulla pubblicazione di un volume e di alcuni articoli relativi alla complessa vicenda di cronaca. L'Ufficio ha rilevato che le pubblicazioni oggetto del reclamo erano in termini generali riconducibili al legittimo esercizio del diritto di cronaca su un fatto di interesse pubblico, ma ha altresì riscontrato che taluni passi indugiavano in una eccessiva esposizione dei dettagli relativi ai rapporti sessuali di taluni degli indagati e dei dettagli relativi alla sfera sessuale della stessa vittima. Pertanto, l'Ufficio ha raccomandato ai titolari del trattamento l'adozione di cautele a tutela dei diritti fondamentali della persona in caso di un'eventuale ristampa o riedizione del libro o di nuove trattazioni del caso in ragione degli sviluppi del procedimento penale in corso (*Nota* 18 febbraio 2009).

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

Anche nel periodo di riferimento il Garante ha ricevuto segnalazioni, reclami e ricorsi riguardanti personaggi “*pubblici*”. Al riguardo, l'Autorità ha ribadito il principio in base al quale esiste un margine più ampio per la diffusione di informazioni che riguardano tali persone, nei limiti dell'interesse pubblico della notizia.

Tra i casi pervenuti si segnala un quesito in merito alla liceità della pubblicazione del dato relativo alla spesa sostenuta per l'uso di un cellulare di servizio da parte di un consi-

Dati relativi
a personaggi
pubblici
e che esercitano
funzioni pubbliche

gliere comunale. L'Ufficio ha osservato che tale pubblicità può ragionevolmente giustificarsi sul piano dell'esercizio legittimo del diritto di cronaca per ragioni di trasparenza sull'uso delle risorse pubbliche. Tale dato, inoltre, può essere lecitamente conosciuto dai terzi, in base alle disposizioni di legge vigenti (art. 59 del Codice e art. 10 del Testo unico delle leggi sull'ordinamento degli enti locali – d.lg. 18 agosto 2000, n. 267; Capo VI l. 7 agosto 1990 n. 241 e succ. modificazioni; *cfr.* anche *deliberazione* del Garante 19 aprile 2007 n. 17 “*Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali*”, in *G.U.* 25 maggio 2007, n. 120 [doc. *web* n. 1407101]). L'Ufficio ha però precisato che il dato, oltre ad essere acquisito lecitamente, deve essere trattato correttamente e, quindi, essere completo e aggiornato.

Il Garante ha poi ritenuto infondata la richiesta di opposizione al trattamento formulata dai dipendenti di un comune che avevano lamentato la pubblicazione, da parte di un quotidiano locale, dei loro nomi e dei compensi che avrebbero ricevuto a titolo di incentivo per la progettazione di un'opera la cui realizzazione era stata sospesa con una sentenza del giudice amministrativo. L'Autorità ha rilevato che le informazioni erano state diffuse senza travalicare i limiti del diritto di cronaca per illustrare un fatto di interesse pubblico nel contesto locale di maggiore diffusione della testata giornalistica. Inoltre, i dati erano contenuti in una determina del segretario comunale lecitamente conoscibile in base alle disposizioni che disciplinano il regime di pubblicità degli atti dell'amministrazione comunale e provinciale (*Prov. 29* maggio 2008 [doc. *web* n. 1531687]).

Sempre in applicazione dei principi sopra ricordati, il Garante ha rigettato una richiesta di opposizione al trattamento, formulata con ricorso da un personaggio noto nel mondo dello spettacolo e della cronaca rosa, in relazione a un'intervista pubblicata su un sito dedicato a un pubblico omosessuale e rilasciata da un giovane che dichiarava di aver avuto una relazione sentimentale con il ricorrente. Il Garante ha ritenuto che l'intervista andava inquadrata nell'ambito di una tematica più generale di interesse pubblico, soprattutto per il pubblico omosessuale (quella relativa al *cd.* “outing”) e le informazioni relative alla sfera privata del ricorrente potevano giustificarsi in considerazione del rilievo che le stesse assumevano rispetto al ruolo e alla vita pubblica del ricorrente medesimo, così come

“costruita” da quest’ultimo attraverso il proprio sito *web*, dichiarazioni e interviste rese pubblicamente (dalle quali emergeva la figura di un attore continuamente agli onori della cronaca per vere e presunte relazioni sentimentali e sessuali con donne) (*Provv.* 2 ottobre 2008 [doc. *web* n. 1559207]).

Il Garante ha esaminato un ricorso con il quale alcuni dirigenti della Rai radiotelevisione italiana S.p.A. hanno lamentato la pubblicazione, da parte di un quotidiano, di un presunto organigramma della Rai medesima in cui compariva una loro asserita appartenenza a una determinata area politica. Il Garante – senza entrare nel merito della questione relativa alla veridicità dell’organigramma e delle informazioni in esso contenute (con i ritenuti, possibili effetti diffamatori), sulla quale si sarebbe potuta eventualmente pronunciare l’autorità giudiziaria – ha rilevato che la pubblicazione è stata effettuata nel quadro del diritto di cronaca e di critica rispetto ad un fatto (l’esistenza di tale organigramma) che costituisce l’elemento essenziale della notizia pubblicata e che si inserisce nell’ampio dibattito, di evidente interesse pubblico, sulla struttura e sull’organizzazione del servizio pubblico radiotelevisivo (*Provv.* 19 maggio 2008 [doc. *web* n.151719] e *Provv.* 30 ottobre 2008 [doc. *web* n.1523831]).

Da segnalare anche la risposta a un quesito in merito alla liceità della pubblicazione, da parte di taluni quotidiani, dei dati relativi agli iscritti a un’associazione massonica. L’Ufficio ha richiamato i principi generali dettati dal codice per i trattamenti effettuati per finalità giornalistiche osservando che i dati in questione possono essere diffusi, anche senza il consenso degli interessati, ma nel rispetto dei limiti posti dall’art. 137 del Codice e, in particolare, di quello dell’ “*essenzialità dell’informazione rispetto a fatti di interesse pubblico*”. Ciò implica una valutazione caso per caso del tipo di dati diffusi e del contesto in cui si essi inseriscono, tenendo conto della “*qualificazione*” dei soggetti menzionati e delle diverse caratteristiche del fatto (*cfr.* artt. 5 e 6 del codice di deontologia). Deve quindi escludersi, in linea di principio, la liceità di una pubblicazione degli elenchi degli iscritti indiscriminata e carente dei presupposti suindicati.

8.5. INFORMAZIONE ON-LINE

Sempre più frequentemente pervengono al Garante segnalazioni per chiedere la cancellazione di dati e immagini personali diffusi e in vario modo reperibili su Internet (*Emule, Youtube, forum, blog*), reputati lesivi della sfera personale dei segnalanti.

L'Autorità non è potuta intervenire quando, da verifiche d'ufficio, è risultato che il titolare del trattamento del sito Internet in questione non risiede in Italia (*v. art. 5 del Codice*). In queste situazioni è stata fornita agli interessati l'indicazione del soggetto titolare, estratto dai registri "*Whois*", cui il segnalante può direttamente richiedere la rimozione immediata dei contenuti ritenuti diffamatori. Ciò, in ottemperanza ad una prassi nota come "*notice and take down*", riconosciuta sia negli Usa sia in ambito comunitario (*cf. Direttiva 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.lg. n. 70/2003*).

Sulle problematiche connesse alla pubblicazione *on-line* degli archivi storici delle principali testate giornalistiche, emerse in occasione di ricorsi presentati all'Autorità, *v. infra, par. 17.2.5*

Social network

Sempre con riferimento al tema Internet, nella 30^{ma} Conferenza internazionale delle Autorità di protezione dei dati personali, tenutasi a Strasburgo nell'ottobre 2008, è stata approvata una "*risoluzione sulla tutela della privacy nei servizi di social network*" che evidenzia come i servizi di *social network*, pur offrendo una gamma del tutto nuova di opportunità comunicative, possono comportare anche rischi per la *privacy* sia degli utenti sia di terzi (*v. infra, par. 20, con riferimento alle conferenze delle autorità su scala internazionale*).

8.6. RETI DI COMUNICAZIONE

8.6.1. Invio di comunicazioni commerciali non sollecitate (spam)

Anche nel corso del 2008 il Garante ha ricevuto diverse richieste d'intervento relativamente ad attività di *spam*.

In diverse occasioni l'Autorità ha vietato l'ulteriore invio di comunicazioni promozio-

nali a terzi senza il consenso preventivo, specifico e informato degli interessati ai sensi dell'art. 130 del Codice, adottando appositi provvedimenti (*Prov. 31 gennaio 2008* [doc. *web* n. 1489843] *Prov. 13 maggio 2008* [doc. *web* n. 1521775] e *Prov. 11 dicembre 2008* [doc. *web* n. 1584213]), talora preceduti da un'attività ispettiva mirata. In tali interventi, il Garante ha inoltre ricordato che un indirizzo *e-mail*, per il solo fatto di essere reperibile in rete, non può essere oggetto di un uso indiscriminato e che occorre ottenere il consenso preventivo del destinatario prima di utilizzare l'indirizzo di posta elettronica per fini di pubblicità e di *marketing*, in quanto la pubblicità di un dato non ne comporta la libera utilizzabilità. In tutti i casi di trattamento illecito per l'invio tramite posta elettronica di comunicazioni non richieste l'Autorità ha comminato le previste sanzioni amministrative.

Il Garante si è occupato del fenomeno dell'invio di *fax* pubblicitari a destinatari che non avevano mai prestato il loro consenso a ricevere tali comunicazioni con diversi provvedimenti di divieto, accompagnati dall'emanazione delle conseguenti sanzioni amministrative, in particolare con *provvedimenti 31 gennaio 2008* [doc. *web* n. 1488781] e *13 maggio 2008* [doc. *web* nn. 1520217, 1520243 e 1520263]. In tali occasioni l'Autorità ha ribadito che la reperibilità dei dati sugli elenchi pubblici, quali ad esempio gli elenchi categorici, non esime il titolare del trattamento, in ragione della specificità del mezzo considerato, dal chiedere il consenso all'interessato per l'uso pubblicitario e commerciale del *telex* in considerazione della specifica disciplina prevista all'art. 130 del Codice.

Il Garante in molti casi, a seguito di complesse istruttorie, ha verificato che l'invio di *fax* avviene da società localizzate all'estero (Francia, Regno Unito e Romania). Pertanto, in questi casi ha provveduto a richiedere la collaborazione delle Autorità competenti dei rispettivi Paesi al fine di far cessare detti invii indesiderati.

In tale contesto è da segnalare il *provvedimento* inibitorio del 19 dicembre 2008 [doc. *web* n. 1580492], con il quale l'Autorità ha disposto il divieto di proseguire il trattamento risultato illecito. In tale caso il Garante ha riscontrato che il consenso non può definirsi "*libero*", quando sia riferito a un ulteriore trattamento dei dati personali che l'interessato

deve acconsentire per conseguire una prestazione richiesta. Gli interessati devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso per ciascuna distinta finalità perseguita dal titolare. Inserendo tra le condizioni generali per la fruizione di un servizio le ulteriori finalità di contatto a fini pubblicitari, i dati personali raccolti lecitamente dal titolare (e conferiti dall'interessato) per l'esecuzione del rapporto contrattuale vengono di fatto piegati a un utilizzo diverso dallo scopo che ne ha giustificato la raccolta, con inevitabile lesione quindi del principio di finalità (art. 11, comma 1, lett. *b*), del Codice).

Il Garante ha ribadito in questa occasione che si deve in ogni caso garantire agli interessati il diritto di esprimere liberamente un valido consenso informato per i trattamenti per finalità di *marketing*, con modalità e in un ambito del tutto distinto da quello relativo al conferimento dei dati indispensabili per dare esecuzione al rapporto contrattuale.

L'Autorità ha partecipato ad una serie di eventi internazionali tra le autorità, e con il supporto dei soggetti privati, per arginare il dilagare del fenomeno dello *spam*. In particolare, il Garante ha preso parte a diverse iniziative del *Cnsa* (*The Eu Contact Network of Spam Authorities*) a Bruxelles e, in tale contesto, è stato presentato uno studio effettuato per la Commissione europea su tutti i Paesi dell'Unione relativamente alle attività avviate per affrontare fenomeni quali *spam*, programmi spia e *software* maligni. Dall'analisi delle iniziative intraprese dalle Autorità competenti e dai fornitori di servizi, nonché delle sanzioni comminate e del livello di cooperazione anche internazionale, il nostro Paese risulta tra i primi sia per impegno sia per risultati raggiunti.

8.6.2. *Banche dati utilizzate per il telemarketing*

A seguito delle numerose segnalazioni pervenute nel 2007 e nel 2008, relative a chiamate indesiderate con finalità promozionali effettuate principalmente da parte delle società telefoniche, il Garante è intervenuto nuovamente sulla materia del *telemarketing*, dopo i provvedimenti del 2007 indirizzati a diversi titolari del trattamento ([doc. *web* nn. 1412626, 1412610, 1412598, 1412557, 1412586] *v. Relazione 2007, p. 83*)).

I provvedimenti inibitori del 2008 [doc. *web* nn. 1544315, 1544326, 1544338, 1562780, 1562758] sono stati diretti non solo nei confronti di società che hanno effettuato tali attività direttamente, o tramite soggetti esterni nominati responsabili del trattamento, ma anche verso alcune tra le primarie società che hanno costituito e hanno venduto le banche dati contenenti le informazioni relative agli interessati da contattare telefonicamente per finalità promozionali.

Ai provvedimenti si è giunti dopo ripetuti richiami, istruttorie e ispezioni effettuate in alcuni casi anche con l'ausilio del Nucleo speciale *privacy*, avviate a seguito di reclami e segnalazioni ricevute dall'Autorità.

Dalla documentazione acquisita nel corso delle predette attività istruttorie, è emerso che le società che hanno fornito i *database* agli operatori telefonici avevano raccolto e ceduto a terzi i dati degli interessati senza informarli (o informandoli in maniera inadeguata) ed anche senza un loro preventivo specifico consenso. Una delle società offriva sul proprio sito i dati di oltre quindici milioni di famiglie italiane suddivise per reddito e stile di vita, senza che gli interessati fossero stati informati o avessero dato il loro assenso alla comunicazione dei dati a terzi.

Da parte loro le aziende e le compagnie telefoniche che hanno acquistato i dati e li hanno utilizzati a fini di *marketing* telefonico (il *cd.* “*teleselling*”), non si sono preoccupate di accertare, come prevede invece la disciplina sulla protezione dei dati, che gli abbonati avessero acconsentito alla comunicazione dei propri dati e al loro uso a fini commerciali.

Successivamente, con l'art. 44, comma 1-*bis* del decreto-legge 30 dicembre 2008, n. 207 (*cd.* “*decreto milleproroghe*”), convertito, con modificazioni, nella legge 27 febbraio 2009, n. 14 (*G.U.* 28 febbraio 2009 n. 49, S.O. 28), è stato stabilito che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.

Di seguito all'entrata in vigore di tale disposizione, che ha introdotto un regime derogatorio e transitorio in materia di *telemarketing*, il Garante ha ritenuto necessario interve-

nire al fine di chiarire rigorosamente i limiti entro i quali le società che operano nel settore possono avvalersi della deroga, precisando altresì le regole che le stesse dovranno seguire nell'uso dei dati degli abbonati.

Con il *provvedimento* del 12 marzo 2009 (G.U. 20 marzo 2009 n. 66 [doc. web n. 1598808]), l'Autorità ha così stabilito che le aziende e i *call center*, che intendano avvalersi della citata deroga e contattare gli utenti per fare promozioni e offerte commerciali utilizzando le predette banche dati, devono innanzitutto documentare in modo adeguato che la banca dati, costituita con i numeri telefonici e gli indirizzi degli abbonati, sia stata effettivamente creata prima del 1° agosto 2005, chiarendo altresì se il trattamento di dati venga effettuato anche per conto terzi. Le società e le aziende del settore, inoltre, sono tenute ad usare questi dati direttamente, senza possibilità di cederli a nessun titolo ad altre aziende.

Gli operatori che telefoneranno agli abbonati dovranno, poi, ad ogni contatto specificare per quale società chiamano e ricordare agli interessati i loro diritti, registrando immediatamente l'eventuale contrarietà dell'abbonato ad essere nuovamente contattato e comunicandogli l'identificativo dell'operatore.

I dati presenti nelle banche dati dovranno essere utilizzati solo a fini promozionali e non potranno in alcun modo essere usati per acquisire nuove informazioni o il consenso degli abbonati ad effettuare chiamate dopo la data del 31 dicembre 2009, poiché ciò determinerebbe di fatto la costituzione di nuove banche dati, andando al di là delle finalità stabilite dalla legge e prorogando, oltre il termine previsto, gli effetti della deroga temporanea.

Il Garante ha infine ricordato che il mancato rispetto del *provvedimento* comporta una sanzione amministrativa che va da 30.000 a 180.000 euro e che, nei casi più gravi, può raggiungere anche i 300.000 euro.

8.6.3. *Telefonia*

Anche nel 2008 diversi comuni hanno evidenziato che le ricerche di persone in pericolo, non in grado di comunicare la propria posizione, ad esempio perché in stato di incoscienza, potrebbero essere agevolate dalla possibilità di ottenere in tempo reale dal competente operatore telefonico la localizzazione del telefono cellulare delle persone stesse. I comuni

richiedenti hanno fatto riferimento all'attività svolta dal Corpo nazionale del soccorso alpino e speleologico (Cnsas), una delle strutture operative del Servizio nazionale della protezione civile (*cf.* art. 11, comma 1, della l. n. 225/1992), che, infatti, ha spesso la concreta necessità di localizzare con urgenza persone disperse, in particolare in zone montane.

Pertanto, con il *provvedimento* del 19 dicembre 2008 [doc. *web* n. 1580543] il Garante ha chiarito che il Codice, nel caso vi sia la necessità di salvaguardare la vita o l'incolumità di una persona, consente alla società telefonica di comunicare senza indugio all'organismo di soccorso, anche senza il consenso dell'interessato, dati quali quelli concernenti i ponti e le celle attivate o "agganciate" dal telefono mobile della persona dispersa. La decisione ha, infatti, ad oggetto solo i dati relativi all'ubicazione diversi dai dati relativi al traffico, ossia i dati che possono essere reperiti sulla rete di comunicazione elettronica a prescindere da una comunicazione tra soggetti.

Pur riguardando il soccorso alpino, il *provvedimento* afferma principi suscettibili di essere applicati, con le dovute cautele, anche in altri casi in cui v'è esigenza di soccorso; l'Autorità ha chiarito, tuttavia, che i dati acquisiti dagli organismi di soccorso dovranno essere utilizzati solo per ricercare e soccorrere la persona dispersa.

L'Autorità ha inoltre ricordato che i servizi abilitati a ricevere le chiamate di emergenza possono comunque trattare i dati relativi all'ubicazione dei telefoni relativi a chi chiama, anche quando l'utente o l'abbonato abbia già rifiutato o omissso di prestare il consenso (*cf.* considerando 36 e art. 10, comma 1, lett. *b*) della Direttiva 2002/58/Ce e art. 127, comma 4, del Codice).