casi, (quando segue la precisazione che l'assenza è per malattia), dati di natura sensibile. Infatti, secondo il costante orientamento del Garante (di recente provv. 10 ottobre 2013, n. 442, doc. web n. 2753605, nonché, negli stessi termini v. provv. 14 giugno 2007, n. 23, doc. web n. 1417809, recante Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 6.3, e Corte di Cassazione 8 agosto 2013, n. 18980) costituisce dato sensibile quello relativo all'assenza dal lavoro di un dipendente per malattia, in quanto tale informazione, pur non facendo riferimento a specifiche patologie, è comunque suscettibile di rivelare lo stato di salute dell'interessato. Pertanto, il Garante ha valutato che l'attribuzione al personale di portineria del trattamento dei dati personali – sensibili e non – degli agenti di polizia penitenziaria in assenza di nomina ad incaricato del trattamento e di definizione dell'ambito di trattamento consentito, configura la violazione dell'art. 30 del Codice (provv. 7 maggio 2015, n. 269, doc. web n. 4167648).

8.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza, anche per il 2015, ha rappresentato l'opportunità di differire l'adempimento delle misure non ancora attuate, tra quelle prescritte dal Garante per rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innovazioni tecnologiche introdotte con l'entrata in funzione del nuovo Sistema di informazione Schengen (SIS II), sia delle difficoltà di realizzazione dei progetti, legate soprattutto alla disponibilità delle necessarie risorse finanziarie. Nel corso dell'anno il Ministero ha peraltro fornito ulteriori elementi, che sono allo stato al vaglio dell'Autorità, circa l'idoneità delle misure poste in essere a soddisfare le prescrizioni impartite.

Su altro profilo, com'è noto il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto).

Il numero ed il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante hanno pertanto, anche quest'anno, subito un lieve calo rispetto all'anno precedente.

Sono invece in lieve aumento le richieste di accesso prevenute al Garante da autorità nazionali di controllo di altri Stati, interpellare dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicare, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62, decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006 del Parlamento Europeo e del Consiglio (cfr. par. 22.4).

9 L'attività giornalistica

L'Autorità è intervenuta su questioni attinenti al bilanciamento fra la libertà di informazione e il diritto alla protezione dei dati personali non solo in occasione del consueto esame di segnalazioni, reclami e ricorsi ma anche mediante la predisposizione di un *report* "La televisione del dolore" presenrato dalla professoressa Licia Califano a Pavia il 24 marzo 2015.

Tale documento ha costituito un'importante occasione di riflessione sul tema e ha, in particolare, evidenziato il divario tra la normativa e il modo di fare informazione da parte di alcuni *media*, talora finalizzato alla "ricerca del sensazionalismo e di un'emotività collettiva usa e getta", attraverso l'uso di immagini e l'indugio su dettagli lesivi della dignità e della sfera privata delle persone (Consiglio nazionale dell'Ordine dei giornalisti – Osservatorio di Pavia *Media Research* – doc. web n. 3845045).

9.1. *Le persone decedute*

I minori

Non è mancata, anche nel periodo di riferimento, la necessità di richiamare gli organi di informazione al rispetto delle particolari garanzie previste per i minori.

In particolare è stata esaminata una segnalazione relativa alle puntate di un programma televisivo dedicate alle indagini concernenti il ritrovamento del cadavere di una donna lungo le rive di un canale e dell'asserita assenza di accorgimenti atti a garantire la vittima ed i suoi congiunti, in particolare i figli minori. Di questi ultimi, infatti, sono state fornite informazioni dettagliate riguardanti la loro vita privata indugiando in particolare sulle diverse ipotesi riguardanti il destino dei minori in caso di un possibile accertamento della colpevolezza del padre. L'Autorità, pur rilevando l'interesse pubblico della vicenda, ha rinvenuto nel trattamento in questione una violazione del limite dell'essenzialità dell'informazione (art. 137, comma 3, del Codice) e delle specifiche garanzie a tutela della dignità e della personalità dei minori previste dal codice di deontologia (art. 7), dalla Carta di Treviso e dalla Convenzione sui diritti del fanciullo (art. 16); conseguentemente ha chiesto all'editore, titolare del trattamenro, di impegnarsi autonomamente a non diffondere ulteriormente i dati personali relativi ai cirari minori, nonché di rimuovere quelli reperibili sulle edizioni *online* (nota 10 luglio 2015).

Gli esiti scolastici

L'Autorità ha poi ricordato che il principio di essenzialità dell'informazione non viene meno per la sola circostanza che i dati da diffondere sono soggetti a un regime di pubblicità, come accade per quelli relativi agli esiti scolastici. Tale assunto è stato richiamato in relazione all'avvenuta diffusione – anche *online* – di una riproduzione del quadro dei voti della classe di cui faceva parte un giovane, deceduto durante una gita scolastica. L'articolo consentiva di individuare i nomi e i cognomi dei compagni di classe del deceduto, associati ai voti ricevuti ivi compresi quelli relativi alla condotta. L'Autorità ha ritenuto che tali informazioni, per la loro natura e per i soggetti a cui si riferivano, nulla aggiungevano al quadro informativo sulle possibili

cause del decesso del giovane e ne ha chiesto pertanto la rimozione (nota 25 giugno 2015).

9.2. *La cronaca giudiziaria*

Vittime di reato

L'Autorità è intervenuta d'urgenza in relazione ad un articolo che, nel dare notizia del rinvio a giudizio dei presunti autori di una violenza sessuale ai danni di una donna, ha diffuso il nome e cognome di quest'ultima unitamente ad altri dati (età, nazionalità, professione del padre), nonché la descrizione particolareggiata delle violenze subire. Nel richiamare i divieti di legge operanti al riguardo (art. 734 c.p.), i limiti previsti dal Codice (art.137, comma 3) e dal codice di deontologia (artt. 6, 8 e 12) a tutela della riservatezza e della dignità della persona e i diversi provvedimenti già adottati in materia (cfr. da ultimo provv. 8 aprile 2009, doc. web n. 1610028) ha disposto il divieto di ogni ulteriore diffusione, anche *online* delle generalità della vittima della violenza descritta, nonché il divieto di diffusione di dati comunque idonei ad identificarla (provv. 18 giugno 2015, n. 358, doc. web n. 4172412).

Immagini del cadavere

Il Garante si è occupato della diffusione delle foto del cadavere di un giovane giornalista ucciso brutalmente dalla camorra nel 1985, pubblicate su un siro internet e su un libro. In particolare, il segnalanre lamentava una violazione della Carta dei doveri del giornalista, dove si dispone che questi "non deve pubblicare immagini o fotografie particolarmente raccapriccianti di soggetti coinvolti in fatti di cronaca, o comunque lesive della dignità della persona, né deve soffermarsi sui dettagli di violenza o di brutalità, a meno che non prevalgano preminenti motivi di interesse sociale" e dell'art. 15 della l. 8 febbraio 1948, n. 47 (Disposizioni sulla stampa). Il Garante ha tuttavia osservato che la pubblicazione di queste foto era giustificata dalla rilevanza sociale rivestita dalle stesse, trattandosi di un fatto di particolare gravità che ha avuto a suo tempo una vasta eco e che ancora oggi, a distanza di trenta anni dall'accadimento del fatto, viene spesso ricordato (provv. 8 ottobre 2015 n. 520, doc. web n. 4363110).

9.3. *I personaggi pubblici*

Dati relativi alla sfera sessuale

Il Garante, pur avendo riaffermato il principio in base al quale la diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni, pur se relative alla sfera privata, può risultare giustificata in ragione della "qualificazione del protagonista" (art. 6, comma 1, del codice deontologico), ovvero del rilievo che le informazioni medesime possono avere sul ruolo o sulla vita pubblica del soggetto cui si riferiscono (art. 6, comma 2), ha ritenuto illecita la diffusione delle descrizioni particolareggiate delle condotte sessuali di una personaggio politico riportate negli scritti confluiti negli atti giudiziari e diffusi negli articoli di stampa cartacea e *online*. Ha infatti applicato l'art. 11 del codice di deontologia, il quale stabilisce che "il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona identificata o identificabile" e che "la pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica" (provv. 8 luglio 2015, n. 407, non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto 2013).

Uso di artifici nelle interviste

Il Garante si è pronunciato nuovamente sulla prassi, adottata in un noto programma radiofonico, di raccogliere telefonicamente dichiarazioni di persone con l'artificio della simulazione di altra identità e successivamente di diffonderle radiofo-

nicamente, sul web o in altro modo. L'Autorità si era già pronunciata in merito con il provvedimento dell'11 settembre 2014, n. 400 (doc. web n. 3405138), ravvisando in tale fattispecie un trattamento illecito di dati personali. Il provvedimento, impugnato, è stato confermato dal Tribunale di Milano (sent. 4 giugno 2015, n. 6968). Ciononostante la prassi descritta è proseguita, sicché l'Autorità, anche alla luce di una nuova segnalazione pervenuta al riguardo, ha ritenuto necessario avviare una nuova istruttoria. Questa si è conclusa con un provvedimento di prescrizione al titolare del trattamento di astenersi dall'acquisizione di dati personali con le modalità descritte, poiché tale condotta costituisce una violazione dei principi di trasparenza e correttezza del trattamento di cui all'art. 11 del Codice e 2 del codice di deontologia.

L'Autorità ha precisato che la prassi descritta configura un vero e proprio "artificio" – non conforme alla menzionata disciplina – consistente non solo nel celare l'identità di giornalista (o soggetto ad esso equiparato ai sensi dell'art. 136 del Codice), bensì anche nell'utilizzare l'identità e la voce di un'altra specifica persona, amica dell'"intervistato" o comunque da questi conosciuta, inducendo così quest'ultimo, fraudolentemente, a manifestare considerazioni del tutto private, confidenziali (talvolta anche dati sensibili) e destinate unicamente, nell'effettivo intento dell'"intervistato", al soggetto del quale il giornalista-imitatore si è artificiosamente assunto l'identità. Ciò, nell'ambito di una conversazione telefonica rispetto alla quale l'interlocutore "intervistato" ha una legittima aspettativa di riservatezza (art. 15 Cost.) (provv. 2 dicembre 2015, n. 631, doc. web n. 4634594).

9.4. *Gli archivi storici e le informazioni* online

In conformità alla sentenza della CGUE del 13 maggio 2014 nel caso Google Spain (cfr. Relazione 2014, p. 87) il Garante è intervenuto a seguito delle segnalazioni e reclami presentate da cittadini avverso il mancato accoglimento da parte di Google delle richieste di deindicizzare pagine presenti sul web riportanti dati personali ritenuti non più di interesse pubblico. Il Garante ha seguito al riguardo i criteri adottati nelle Linee guida del Gruppo Art. 29 (parere WP 26 novembre 2014, n. 225, doc. web n. 3876849).

Tra i casi di accoglimento, si segnala quello relativo ad un articolo rinvenibile tra l'elenco dei risultati generato da Google a seguito della ricerca effettuata a partire dal nome e cognome dell'interessato riguardante i dissidi intercorsi tra il segnalante e l'autore di un *blog* in costanza di un rapporto professionale da tempo interrotto. Il Garante ha ritenuto i fatti rinvenibili nella url privi di inreresse pubblico e ne ha prescritto a Google la rimozione a partire dal nome e dal cognome del segnalante (provv. 16 aprile 2015, n. 222, doc. web n. 4006340).

Ha inoltre ritenuto di prescrivere a Google la rimozione di un articolo del 1999 che dava conto della visita effettuata dal segnalante, all'epoca deputato, a un detenuto presso un carcere nel reparto speciale riservato ai mafiosi. A seguito di tale incontro, la Procura antimafia avrebbe aperto un'indagine per verificare se la visita fosse stata effettivamente solo mirata a controllare le "condizioni generali della detenzione" come prescritto dalla legge per i parlamentari.

Il Garante ha ritenuto la lesione provocata dall'indicizzazione dell'articolo in questione sproporzionata in ragione del rilevante lasso di tempo trascorso dalla vicenda e delle dichiarazioni del segnalante secondo le quali non è stato avviato alcun procedimento penale nei suoi confronti (provv. 5 febbraio 2015, n. 64, doc. web n. 3793836).

Il Garante, invece, non ha accolto le richieste relative a controversie giudiziarie ancora in corso, di rilevanza nazionale (provv.ti 8 gennaio 2015, n. 1, doc. web n. 3730791, 16 aprile 2015, n. 224, doc. web n. 4006473 e 4 giugno 2015, n. 335 doc. web n. 4172122), strettamente connesse all'attività professionale dei reclamanti (provv. 16 aprile 2015, n. 223, doc. web n. 4006413), particolarmente efferate (provv. 16 aprile 2015, n. 225, doc. web n. 4006601) e quindi caratterizzate da un persistente interesse pubblico alla loro rinvenibilità sul motore di ricerca.

Deindicizzazione dei nominativi su atti ministeriali pubblicati su GU *online*

Il Ministero della giustizia ha riferito di avere ricevuto numerose richieste di oscuramento dei nomi di persone riportati su atti ministeriali – segnatamente decreti per riconoscimento dei titoli professionali conseguiti all'estero pubblicati nella GU *online*. In particolare gli interessati si lamentavano della circostanza che le ricerche condotte sul web mediante i comuni motori di ricerca consentivano di risalire ad atti pubblicati nella GU anche a notevole distanza di tempo. Il Garante, richiamando le Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, adottate dal Garante con provv. 15 maggio 2014, n. 243 (doc. web n. 3134436), la menzionata sentenza della CGUE e le cit. Linee guida adottare dal Gruppo Art. 29 (doc. web n. 3134436), ha rappresentato l'opportunità che l'Amministrazione, alla luce dei criteri della notorietà pubblica dell'interessato e della risalenza nel tempo dell'informazione, valuti la sussistenza di motivi che giustifichino l'indicizzazione, da parte dei motori di ricerca, dei dati personali citati nei provvedimenti pubblicati nella GU *online*, adottando, se del caso, gli accorgimenti tecnici opportuni per impedire l'indicizzazione stessa (nota 14 dicembre 2015).

10 Il trattamento di dati personali attraverso internet

10.1. *L'informativa e consenso per il trattamento dei dati personali mediante i siti web*

Come già segnalato l'anno scorso (cfr. Relazione 2014, p. 89), l'Ufficio ha ravvisato per alcuni siti web profili di parziale inidoneità in ordine ad alcune informative rilasciare ai sensi dell'art. 13 del Codice nonché con riguardo a *form* di registrazione a servizi vari per consensi non adeguatamente differenziati a seconda dei diversi trattamenti di dati indicati o, in alcuni casi, impostati in maniera da essere obbligatoriamenre resi per finalità ulteriori a quelle di servizio, ai sensi degli artt. 23 e 130 del Codice.

In materia, si segnala l'adozione del provvedimento 1° ottobre 2015, n. 508 (doc. web n. 4452896) a contenuto inibitorio e prescrittivo, adottato in relazione all'invio di messaggi promozionali indesiderati via sms ad utenti che avevano prestato il proprio consenso al solo scopo di ottenere l'iscrizione ad un servizio di candidatura *online* per la ricerca di lavoro.

Inoltre, può farsi riferimento anche al provvedimento 18 novembre 2015, n. 605 (doc. web n. 4487559) adottato nei confronti di una nota società di *e-commerce,* la quale rilasciava un'informativa priva del riferimento ad alcune operazioni di trattamento (come la profilazione e la comunicazione a terzi per finalità promozionali) che, secondo quanto accertato, effettuava e raccoglieva un consenso preselezionato e unico al trattamento dei dati (v. *amplius* par. 11.3).

10.2. *Le Linee guida in materia di trattamento di dati personali per profilazione* online

Nel mese di marzo, in coerenza con le regole emanate nei confronti di Google Inc., di cui al provvedimento 10 luglio 2014, n. 353 (doc. web n. 3283078), il Garante ha adottato un provvedimento a carattere generale volto a disciplinare l'attività dei soggetti che, offrendo servizi *online* accessibili al pubblico attraverso reti di comunicazione elettronica (i cd. servizi della società dell'informazione), effettuano anche attività di profilazione ovvero di analisi ed elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", cioè in gruppi omogenei per comportamenti o caratteristiche sempre più specifici.

L'Autorità, con l'intento di armonizzare e semplificare le regole applicabili in materia di protezione dei dati personali nell'espletamento di questa attività, generalmente strumentale sia alla messa a disposizione di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente, sia alla fornitura di pubblicità personalizzata, ha richiamato i titolari all'adempimento di specifici obblighi, ed innanzitutto quello di fornire agli utenti un'informativa chiara e completa, facilmente accessibile, preferibilmente strutturata su più livelli.

In secondo luogo, ha ricordato la necessità di richiedere ed ottenere il consenso degli interessati, revocabile in ogni momento, per la profilazione per finalità promozionali comunque effettuata: sia se relativa al trattamento, in modalità automatizzata, dei dati personali che derivano dall'utilizzo di servizi di posta elettronica; sia se fondata sull'incrocio dei dati raccolti in telazione alla fornitura ed al relativo utilizzo

di più servizi diversi tra quelli messi a disposizione dell'utente (ad es., posta elettronica e navigazione sul web, partecipazione a *social network* e utilizzo di mappe o visualizzazione di contenuti audiovisivi etc.); sia, infine, se basata sul ricorso ad altre tecniche di identificazione (credenziali di autenticazione, *fingerprinting*, etc.).

L'Autorità ha inoltre imposto modalità di trattamento idonee ad offrire concrete tutele tanto agli utenti, cd. autenticati, che accedono ai servizi tramite un *account* (ad es., per l'utilizzo della posta elettronica), quanto a quelli che ne fanno uso in assenza di preventiva autenticazione, come in caso di semplice navigazione *online*.

Pur ribadendo la libertà di scelta che compete ai titolari, le Linee guida varate dal Garante hanno fornito anche alcune indicazioni pratiche circa le misure da adottare per assicurare la conformità alla normativa dei trattamenti di dati in questione.

A tale scopo è stata, tra l'altro, identificata una possibile modalità per l'acquisizione del consenso *online* che prevede la presentazione di un *banner* all'utente attraverso il quale questi possa attivamente effettuare scelte consapevoli sul trattamento delle informazioni che lo riguardano. Si tratta di un meccanismo che, a tecnologia vigente e in una prospettiva di semplificazione, presenta vantaggi sia in termini di tutela della persona sia di salvaguardia della sua esperienza di navigazione o di accesso ad altri servizi in rete.

Da ultimo, è stato ribadito l'obbligo, che grava sui titolari, del rispetto del diritto di opposizione previsto dal Codice, nonché quello dell'adozione di una *policy* per la definizione di tempi di conservazione dei dati che risultino proporzionati alle specifiche finalità perseguite (provv. 19 marzo 2015, n. 161, doc. web n. 3881513).

10.3. *La consultazione pubblica su* Internet of Things

Con provvedimento 26 marzo 2015, n. 179 (doc. web n. 3898704), l'Autorità ha avviato una consultazione pubblica sul cd. *Internet of Things* (IoT), segnatamente sui rischi per la protezione dei dati che derivano dall'impiego sempre più generalizzato di tecniche che consentono l'interazione e l'interconnessione di oggetti e sistemi diversi (*smartphone*, *tablet* e pc, ma anche oggetti di uso quotidiano come, tra gli altri, dispositivi indossabili, di automazione domestica e di geolocalizzazione e navigazione assistita).

Gli accorgimenti tecnici utilizzati consentono infatti, per il tramite di sensori integrati negli oggetti, di registrare, processare, immagazzinare dati localmente o tramite l'interoperabilità dei dispositivi tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es., Rfid e *bluetooth*), sia tramite una rete di comunicazione elettronica. Ne risultano spesso vantaggi e semplificazioni d'uso per l'utente (impianti di riscaldamento che si accendono da remoto con lo *smartphone*, frigoriferi che segnalano la scadenza dei cibi, sistemi di trasporto in grado di aumentare automaticamente il numero delle corse sulla base degli accessi registrati ai tornelli, orologi intelligenti che segnalano al medico curante eventuali anomalie corporee, sistemi di allarme che si azionano in modo autonomo, luci per uso pubblico o privato che si azionano rispettando parametri di funzionalità e risparmio energetico), che tuttavia comportano la raccolta, la registrazione e l'elaborazione di una grande quantità di informazioni relative a utenti spesso inconsapevoli.

Questi dati consentono non solo di costruire profili dettagliati delle persone, basati sui loro comportamenti, abitudini, gusti e perfino sullo stato di salute, ma di effettuare anche un monitoraggio particolarmente invasivo sulla loro vita privata e di mettere in atto potenziali condizionamenti della loro libertà, peraltro basandosi

10

su informazioni delle quali non è neppure possibile garantire l'affidabilità o il trattamento nel rispetto di rigorose misure di sicurezza.

L'avvio della consultazione pubblica ha avuto l'obiettivo di effettuare una valutazione complessiva anche allo scopo di definire misure per assicurare agli utenti la massima trasparenza nell'uso dei loro dati personali e per tutelarli contro possibili abusi. In particolare, con lo strumento della consultazione pubblica, l'Autorità ha inteso acquisire elementi e proposte sulle modalità di informazione degli utenti, anche in vista di un eventuale consenso; sulla possibilità che fin dalla fase di progettazione dei servizi e dei prodotti gli operatori coinvolti adottino soluzioni tecnologiche a garanzia della *privacy* degli utenti (in un'ottica di cd. *privacy by design*); sul ricorso a tecniche di cifratura e anonimizzazione delle informazioni; sulla interoperabilità dei servizi e sugli aspetti di standardizzazione necessari per garantirla; sull'adozione di strumenti di certificazione.

Conclusa, nel novembre 2015, la fase di acquisizione dei contributi, è attualmente in corso la loro valutazione da parte dell'Autorità.

11 Il trattamento di dati personali nel settore delle comunicazioni elettroniche

11.1. *Le telefonate promozionali indesiderate*

Anche nell'anno di riferimento l'Autorità ha dovuto svolgere complesse attività istruttorie per contrastare il fenomeno delle chiamate indesiderate. Ciò, in quanto il flusso delle segnalazioni pervenute è, rispetto agli anni precedenti, ulteriormente cresciuto. Innanzitutto, per determinate la riconducibilità delle chiamate agli effettivi autori delle telefonate in questione, si è dovuto procedere a degli specifici accertamenti. Tale indagine è stata assai più complessa nei numerosissimi casi in cui le chiamate sono state fatte mediante l'oscuramento delle numerazioni chiamanti. Inoltre, dalle suddette verifiche si è constatato che le aziende pubblicizzanti i prodotti si sono avvalse, oltre che del proprio personale, anche di agenzie esterne le quali a loro volta hanno demandato l'operato a terzi soggetti a volte anche stabiliti all'estero. Al riguardo, nel corso di alcuni accertamenti ispettivi presso le aziende committenti, nonché in occasione di riunioni in sede con alcuni gestori telefonici, è stato riscontrato che le filiere di soggetti cui vengono demandate le attività di *telemarketing* sono talmente diramate per l'uso ripetuto di agenzie e *sub* agenzie da non consentire sempre agli stessi soggetti mandanti il controllo della struttura e diventando quindi difficile risalire a coloro che materialmente hanno effettuato i contatti telefonici lamentati, nonché alle numerazioni chiamanti.

Come sopra evidenziato, il fenomeno del cd. oscuramento ha assunto, nel tempo, dimensioni sempre più considerevoli in materia di *telemarketing* "selvaggio". L'impossibilità, per l'utente, di indicare la numerazione chiamante nelle segnalazioni ha reso difficile, in tali casi, l'individuazione del titolare e quindi l'accertamento della sussistenza della violazione della disciplina relativa alla protezione dei dati personali.

L'Autorità ha dunque deciso di affrontare tale fenomeno adottando misure più rigorose nell'ambito dei poteri che le sono attribuiti dal Codice riuscendo a risalire ai numeri chiamanti nonostante l'oscuramento.

Si segnala in particolare l'adozione di un provvedimento di divieto e prescrittivo nei confronti di una società di *telemarketing* (provv. 1° ottobre 2015, n. 503, doc. web n. 4449190). Si tratta del caso di un utente che lamentava di essere stato disturbato con offerte promozionali nonostante il proprio numero non fosse presente, come da sua richiesta, in alcun elenco telefonico (cd. utenza riservata). Il segnalante non possedeva un dispositivo che consentisse la visualizzazione del numero da cui lo contattavano i promotori commerciali e aveva potuto fornire all'Autorità solo generiche indicazioni sulle chiamate ricevute. Per poter accertare i fatti segnalati, il Garante ha dovuto quindi avviare diverse verifiche con più operatori telefonici che hanno permesso di risalire alla numerazione chiamante, riconducibile a una società di *telemarketing* nei confronti della quale è poi stato adottato il suddetto provvedimento unitamente alla società committente.

Si rappresenta, infine, che numerose istruttorie avviate sono state definite con la contestazione di sanzioni nei confronti sia delle società committenti, sia di quelle delegate direttamente o indirettamente all'effettuazione di attività di *telemarketing*.

11.2. *I trattamenti di dati personali effettuati mediante* call center *ubicati al di fuori dell'Unione europea*

A seguito delle prescrizioni impartite con il provvedimento 10 ottobre 2013, n. 444 (doc. web n. 2724806), sono pervenute al Garante nel 2015 diverse notificazioni di trasferimento o affidamento all'estero del trattamento di dati personali per servizi di *call center*.

Inoltre è proseguita l'attività ispettiva già avviata negli anni scorsi, in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza, per verificare la liceità dei trattamenti posti in essere dai titolari che si avvalgono di *call center* esteri. Sono state sottoposte ad accertamento ispettivo 29 società, tra titolari del trattamento e *call center* che operano in qualità di responsabili. Ne è emerso un quadro di sostanziale conformità alla disciplina.

Inoltre, il Garante e la competente Istituzione albanese hanno siglato il 10 febbraio 2015 un Accordo di cooperazione allo scopo di assicurare la tutela dei dati personali dei cittadini italiani e albanesi raccolti e utilizzati da soggetti pubblici e privati che operano in Albania, dove negli ultimi anni molte aziende italiane hanno fatto richiesta di servizi di *call center*.

La cooperazione prevede un'attività ispettiva congiunta presso pp.aa. e aziende private, inclusi i *call center* che operano in Albania (doc. web n. 3733348).

11.3. *I dati personali utilizzati a fini di* marketing *e profilazione*

In materia di *marketing* e profilazione, con specifico riferimento ai trattamenti di dati effettuati da una società fornitrice del servizio di posta elettronica certificata, l'Autorità ha vietato il trattamento dei dati personali raccolti al momento della sottoscrizione del contratto relativo alla richiesta di attivazione del servizio di posta elettronica certificata, per ulteriori finalità (quali quelle promozionali, di profilazione e comunicazione a soggetti terzi autonomi titolari del trattamento), poiché non conforme a quanto previsto dagli artt. 23 e 130 del Codice. Inoltre, ha prescritto di adottare, qualora intenda raccogliere dati personali degli interessati ed utilizzarli per finalità di definizione del profilo dell'utente e/o di promozione commerciale, le misure necessarie ed opportune al fine di rendere i trattamenti dei dati personali conformi alla normativa in materia e, in particolare, l'acquisizione di specifici consensi al trattamento dei dati personali per ciascuna distinta finalità eterogenea. Si evidenzia altresì che l'Autorità ha prescritto, per quanto riguarda il *form* di contatto per la richiesta d'assistenza, l'eliminazione di qualsivoglia meccanismo di subordinazione dell'esito della procedura alla prestazione di un consenso per il trattamento di dati personali a fini promozionali o di definizione del profilo dell'utente e, qualora intenda utilizzare i dati otrenuti per le comunicazioni di cui all'art. 130, comma 4, del Codice, l'adeguamento alle previsioni di quest'ultimo (ossia il cd. "*soft spam*"). È stato chiesto infine di inserire nell'informativa relativa al *form* un chiaro ed espresso riferimento all'art. 130, comma 4, del Codice ove intenda trattare i dati ottenuti in conformità a tale disposizione, specificando, altresì, le diverse finalità perseguite e chiarendo il tipo di modalità di comunicazione promozionale utilizzata (automatizzata e non automatizzata) (provv. 13 maggio 2015, n. 291, doc. web n. 4337465).

L'Autorità inoltre è intervenuta nei confronti di una delle più importanti società di fornitura *online* di biglietti per spettacoli teatrali, manifestazioni sportive, concerti, nonché di *e-commerce* di prodotti anche di marchi celebri. Dagli accertamenti

ispettivi svolti è emerso che la società raccoglieva dati personali attraverso tre siti web, di cui uno operativo in più lingue straniere destinato ad utenti di Paesi UE ed *extra*-UE, talora richiedendo un consenso preselezionato e unico per varie finalità, fra cui quelle di *marketing*, profilazione, nonché comunicazione dei dati ad altre società, per le loro autonome finalità commerciali. In particolare, la società svolgeva un'attività di profilazione utilizzando un *software* per l'invio di *newsletter* personalizzate, "create" elaborando i dati relativi agli ordini dei clienti o anche a prodotti inseriti nel carrello il cui ordine non era stato comunque finalizzato, senza aver provveduto a notificare all'Autorità siffatto invasivo trattamento.

Il Garante, pertanto, ha vietato alla stessa, ai sensi dell'art. 23 del Codice, l'illecito trattamento dei dati personali di oltre trecentomila clienti, altresì prescrivendole di integrare l'informativa, resa *online*, indicando le aziende o le categorie economiche o merceologiche, alle quali intende comunicare i dati per finalità promozionali. Ha inoltre prescritto alla medesima società di avvisare le aziende, alle quali i dati erano stati comunicati o ceduti, di non utilizzarli senza il consenso degli interessati, nonché di prevedere tempi di conservazione dei dati e di provvedere all'immediata cancellazione o alla anonimizzazione permanente degli stessi alla scadenza del termine di conservazione (provv. 18 novembre 2015, n. 605, doc. web n. 4487559).

11.4. *Le verifiche preliminari* ex *art. 17 del Codice*

Il Garante nel corso dell'anno ha analizzato e dato riscontro a più verifiche preliminari presentate da titolari del trattamento afferenti a diversi settori produttivi, ossia a specifiche istanze volte a individuare misure ed accorgimenti idonei ad assicurare la correttezza e la liceità dei trattamenti prima della loro effettuazione, in considerazione dei rischi specifici per il diritto alla protezione dei dati personali degli interessati.

I mutamenti registrati nel mercato della telefonia ed in particolare la crescente richiesta di servizi personalizzati, sotto il profilo dei contenuti e del piano tariffario, hanno indotto alcuni fornitori di servizi di comunicazione elettronica accessibili al pubblico a richiedere all'Autorità, attraverso istanze di verifica preliminare (*ex* art. 17 del Codice), l'autorizzazione allo svolgimento di ulteriori trattamenti di dati personali aggregati della propria clientela per finalità di profilazione, previo esonero dall'acquisizione del consenso specifico degli interessati (*ex* art. 24, comma 1, lett. *g*) del Codice), ferma restando la necessaria acquisizione del consenso preventivo degli stessi per la successiva attività di *marketing* diretto (art. 23 del Codice).

Settore telefonico

Tenuto conto dei provvedimenti generali 25 giugno 2009 (doc. web n. 1629107) e 6 febbraio 2014 (doc. web n. 2951718), nonché degli specifici provvedimenti emanati in tale ambito a seguito di precedenti istanze di *prior checking*, il Garante ha adottato due provvedimenti prescrittivi nei confronti di due operatori telefonici coinvolti, stabilendo una serie di misure giuridiche e di accorgimenti tecnici volti a garantire il corretto trattamento dei dati personali aggregati dei clienti, nel contesto di più articolati *cluster* di utenza che consentono il passaggio da un modello di analisi statico, incentrato sui servizi e prodotti telefonici offerti, ad un modello più dinamico volto a comprendere ed a valorizzare le nuove esigenze della clientela. In entrambi i provvedimenti sono state previste specifiche misure di sicurezza rispetto al trattamento dei dati aggregati della clientela ai fini della composizione dei *cluster* di utenti, nonché specifiche prescrizioni rispetto all'informativa da rilasciare agli stessi ai sensi dell'art. 13 del Codice, alle moda-

11

lità per consentire l'opposizione degli interessati, in tutto o in parte, al trattamento dei propri dati in maniera celere ed agevole, nonché alla conservazione dei dati ed alla loro successiva cancellazione, ovvero anonimizzazione (provv.ti 15 ottobre 2015, n. 534, doc. web n. 4541143 e 17 dicembre 2015, n. 663, doc. web n. 4698620).

Carte fedeltà

In relazione all'attività di profilazione e *marketing*, in particolare nel settore delle carte fedeltà, sono state sottoposte all'Autorità, anche ai sensi del provvedimento generale 24 febbraio 2005 (doc. web n. 1103045), alcune istanze di verifica preliminare. Una è stata presentata da parte di una società promotrice di un programma di fidelizzazione basato sulla raccolta dei dari personali di frequentarori di sale bingo detentori di carte fedelrà. Con l'istanza in questione è stato chiesto al Garante di valutare il possibile rilascio di un'autorizzazione in merito alla conservazione dei dati personali dei clienti per finalità di profilazione e *marketing* per un periodo superiore ai 12 e 24 mesi fissati nel richiamato provvedimento generale, indicato dalla società in cinque anni.

L'Autorirà, considerate le particolati caratteristiche degli interessati fruitori dei servizi resi, i quali più agevolmente che in altri settori possono essere distinti in frequentatori abituali ovvero occasionali delle sale bingo, ha provveduto ad un accoglimento parziale della richiesta a seguito di un bilanciamento degli interessi dei soggetti coinvolti. Ha pertanto reputato congruo un periodo massimo di conservazione dei dati utilizzati dalla società titolare per attività di profilazione della clientela pari a 12 mesi, con l'aggiunta di un ulteriore periodo non superiore a tre mesi per consentire l'eventuale monitoraggio e la profilazione effettuata in relazione a eventi annualmente ricorrenti. Ha poi consentito, alla società di beneficiare di modalità di cancellazione dei dati che non necessitino di un aggiornamento con cadenza quotidiana, certamente più onerose, ma che possano essere effettuate anche per periodi e dunque a blocchi, purché non superiori ad un trimestre.

Con riguardo ai successivi trattamenti effettuati pet finalità di *marketing*, è stato infine ritenuto congruo autorizzare la conservazione dei relativi dati per un periodo non superiore a 24 mesi (provv. 2 luglio 2015, n. 394, non pubblicaro ai sensi dell'art. 24 reg. Gatante 1° agosto 2013).

All'Autorità è stata presentata, inoltre, un'istanza di verifica preliminare da parte di una società promotrice di un noto programma di fidelizzazione ai fini dell'autorizzazione a conservare i dati dei clienti, detentori della carta fedeltà, per finalità di profilazione e *marketing* per un periodo superiore a quello fissato nel menzionato provvedimento generale. L'istanza ha in particolare riguardato la possibilità di utilizzare, a fini di profilazione aggregata, i dati delle operazioni effettuate da detentori della carta che non avessero fornito il consenso alla profilazione individuale, nonché la possibilità di ottenere, dai soggetti interessati, un consenso unico per le attività di profilazione e di correlato *marketing* mirato.

L'Autorità, ha stimato congruo un periodo massimo di conservazione dei dati utilizzati dall'istante per attività di profilazione individuale e *marketing* della clientela di 24 mesi e, per attività di profilazione aggregata, di 36 mesi, disponendo che, alla relativa scadenza, i dati vengano cancellati in modo automatico e non reversibile. Ha inoltre disposto specifiche e stringenti misure giuridiche e tecniche per garantire il corretto trattamento dei dati dei detentori della carta fedeltà per finalità di profilazione aggregata (nello specifico analisi di macro fenomeni relativi a *trend* generalizzati di consumo rispetto a determinate categorie merceologiche) senza l'acquisizione dello specifico consenso degli stessi, in forza di un bilanciamento di interessi operato ai sensi del cit. art. 24 del Codice. Il Garante ha invece escluso la possibilità di ricorrere all'acquisizione di un consenso unico per finalità di profilazione

e correlato *marketing* mirato, richiamando il chiaro disposto dell'art. 23 del Codice ed esteso anche a tali ambiti le previste misure di sicurezza, oltre che disposto altri accorgimenti avuto riguardo al modello di informativa da rendere agli interessati, ai sistemi ed alle banche dati utilizzati dalla società, nonché al trasferimento dei dati all'estero (provv. 15 gennaio 2015, n.17, non pubblicato ai sensi dell'art. 24 reg. Garante 1° agosto 2013).

Media

Il Garante si è pronunciato su due istanze di *prior checking* presentate da società operanti nel settore dei *media* nell'ambito del medesimo gruppo, sempre rispetto al trattamento di dati personali degli utenti per finalità di profilazione e *marketing*.

La prima istanza si riferiva alla raccolta in forma aggregata ed al monitoraggio di dati di visione generati dai telespettatori nell'ambito di un servizio che consente di rivedere i programmi televisivi riferibili alla programmazione settimanale di alcune specifiche reti televisive, fruibili in digitale terrestre o via internet attraverso l'utilizzo di dispositivi *set-top box* o *smart* tv, su cui vengono scaricate le applicazioni.

La seconda istanza si riferiva all'analisi aggregata di informazioni relative alla visione di appositi canali *tv pay* e *free* sia della società istante, sia generalisti, attraverso televisori e *decoder* (associati ad un numero di *smartcard*) predisposti per una connessione alla rete internet. In entrambi i casi i trattamenti erano rivolti all'analisi delle prestazioni del servizio per migliorare l'offerta rendendola più aderente ai gusti del pubblico televisivo e i dispositivi utilizzati erano caratterizzati dalla presenza di un codice identificativo univoco, sottoposto ad apposite tecniche di *hashing*, al fine di non consentirne l'intellegibilità. In considetazione di tale circostanza l'Autorità, dopo una complessa attività istruttoria, ha avuto modo di precisare che i processi di cifratura applicati a tali codici consentivano comunque di mantenere una univocità di corrispondenza tra dato originario e dato cifrato e che pertanto era possibile, individuando i dispositivi ad essi associati, risalire anche indirettamenre all'utente televisivo.

Conseguentemente, entrambe le società hanno integrato i propri sistemi tecnici e previsto l'utilizzo dei dati dei telespettatori e dei codici identificativi dei dispositivi dopo aver acquisito il consenso preventivo degli stessi. Nel quadro delineato l'Autorità ha pertanto previsto, in entrambi i provvedimenti l'adozione di una serie di misure relative al corretto rilascio dell'informativa agli utenti, alle modalità concrete di esercizio dei diritti di cui all'art. 7 del Codice ed in particolare del diritto di revoca del consenso rilasciato dal telespettatore, nonché alla conservazione dei dati (provv.ti 12 marzo 2015, n. 144, doc. web n. 3881392 e 23 aprile 2015, n. 241, doc. web n. 4015426).

Alta moda

Il Garante ha adottato un provvedimento prescrittivo a seguito di un'istanza di verifica preliminare presentata da una società di alta moda, al fine di profilare la propria clientela per offrire servizi specifici ed effetruare attività promozionali personalizzate (cd. *marketing* profilato) mediante la conservazione e il trattamento dei dati personali dei propri clienti per un periodo superiore a quello previsto di 12 e 24 mesi (cfr. cit. provv. generale 24 febbraio 2005). Si ricorda che già negli ultimi anni il Garante aveva adottato provvedimenti simili riguardanti il medesimo settore (provv.ti 30 maggio 2013, n. 263, doc. web n. 2547834; 7 novembre 2013, n. 500, doc. web n. 2920245 e 24 aprile 2013, n. 219, doc. web n. 2499354). Nella richiesta pervenuta, la società ha prospettato un tempo di conservazione dei dati personali pari a dieci anni. Il Garante (ricordando che tali attività necessitano, comunque, del consenso degli interessati) ha titenuto di prescrivere come congruo un periodo di conservazione di sette anni (analogamente a quanto stabilito nei due cit. provv.ti del 2013), in relazione sia alle finalità prospettate, sia alla tipologia di dati personali oggetto di trattamento. Inoltre, ha reputato i menzionati termini di con-

servazione adeguati ai rischi degli interessati, in quanto trattandosi di beni di cd. "fascia alta", i cui acquisti vengono effettuati di massima una o due volte l'anno, un periodo inferiore di conservazione avrebbe reso, di fatto, inutile la profilazione. Il Garante, dunque, ha impartito specifiche e puntuali prescrizioni alla società che, quindi, potrà effettuare attività di profilazione e *marketing* profilato solamente previo consenso specifico dell'interessato e adottando ulteriori misure quali apposite procedure di autenticazione ed autorizzazione, obbligarorierà del tracciamento dei *log* di accesso a ciascun sistema informatico per sei mesi (in modo da realizzare un controllo analitico *ex post* delle attività svolte dai singoli incaricati). Peraltro, la società potrà conservare i dati personali della propria clientela solo per il periodo individuato nel provvedimento (sette anni), al termine del quale dovrà provvedere alla cancellazione automatica dei dati, ovvero alla loro permanente trasformazione in forma anonima (provv. 2 dicembre 2015, n. 632, doc. web n. 4642844).

11.5. *Il* mobile ticketing

Come riferito nella Relazione 2014 (cfr. p. 96), in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, il Garante ha adottato un provvedimento generale sul *mobile remote payment* (provv. 22 maggio 2014, n. 258, doc. web n. 3161560), riservandosi di intervenire con ulteriori provvedimenti anche nel settore dell'offerta e dei pagamenti di titoli digitalizzati per l'accesso a servizi di utilità sociale o in mobilità. In tal senso, tenuto conto del quadro normativo vigente (in particolare d.l. n. 179 del 18.10.2012, cd. "Decreto sviluppo-*bis*", convertito con modificazioni nella l. n. 221 del 17.12.2012, della l. n. 147 del 27.12.2013, anche in considerazione della successiva l. n. 124 del 07.08.2015), dopo aver svolto un'attività conoscitiva in tali ambiti, ha avviato, con provvedimento 10 settembre 2015, n. 467 (doc. web n. 4273074), una pubblica consultazione su uno schema di provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di *mobile ticketing* che prevede una serie di tutele per garantire agli interessati che vogliano acquistare, via sms, biglietti dell'autobus o dei parcheggi o fruire con tale modalità di servizi di *car sharing* o *bike sharing*, oppure accedere ad aree a traffico limitato. Ciò, nell'ottica di fornire un quadro organico di regole rivolte a tutti i soggetti coinvolti, come i soggetti che offrono servizi per la mobilità e il trasporto nelle aree urbane ed extraurbane, i nuovi operatori di matrice non bancaria come gli operatori di telecomunicazioni, gli *hub* tecnologici che forniscono la piattaforma tecnologica per la distribuzione ed il pagamento dei *ticket* digitali, nonché i soggetti che gestiscono circuiti di intermediazione e gli operatori bancari, laddove l'operazione di pagamento preveda la registrazione ad un apposito sito web, nonché la titolarità di uno strumento di pagamento tradizionale come la carta di credito.

11.6. *Il contrasto allo* spam

Nel corso dell'anno sono state numerose le segnalazioni riguardanti la ricezione di comunicazioni indesiderate con modalità automatizzate, in particolare tramite *e-mail*, e, in misura decisamente minore, tramite sms e fax. L'Autorità ha proseguito nell'attività di contrasto allo *spam*, analizzando i casi segnalati e avviando varie istruttorie con riferimento ai trattamenti oggetto di segnalazioni più numerose oppure con profili di maggiore criticità, come invio di comunicazioni indesiderate

anche dopo l'opposizione al trattamento e/o la difficoltà degli interessati nell'esercizio dei diritti di cui agli artt. 7 ss. del Codice.

In molti casi, è risultato difficile individuare i titolari del trattamento, sia per le modalità con cui si può operare in rete, sia perché talora i siti mittenti risultano intestati a soggetti fantasiosi o comunque privi di recapiti utilmente contattabili, sia perché spesso essi hanno sede in Paesi (anche extraeuropei), ove l'Autorità non ha competenza (v. art. 5 del Codice).

Al riguardo, va però ribadito che 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, non solo in termini di disciplina sostanziale ma anche per quanto attiene alle tutele azionabili, con particolare riferimento alla tipologia di soggetti tutelati dagli ordinamenti in questo specifico ambito (persona fisica, persona giuridica, enti, associazioni ...). Differenze che, si auspica, verranno eliminate o comunque attenuate con l'entrata in vigore e l'implementazione del nuovo regolamento UE in materia di protezione dei dati personali, almeno riguardo a profili essenziali quali i soggetti aventi diritto alle tutele previste dalla normativa in materia di prorezione dei dati, i diritti tutelabili presso le Autorità nazionali preposte, i criteri di raccordo fra le competenze di tali Autorità (qualora si tratti di trattamenti di dati che interessino più ordinamenti nazionali) (cfr. par. 22.3).

Si segnalano, in materia, i provvedimenti 18 novembre 2015, n. 605 (doc. web n. 4487559) e 13 maggio 2015, n. 291 (doc. web n. 4337465) relativi alla modifica della formula di acquisizione del consensi per la finalità di *marketing* in sede di raccolta dei dati, quale attività spesso propedeutica all'invio di comunicazioni promozionali indesiderate e quindi alla produzione di *spam* (cfr. par. 11.3).

11.6.1. Trattamento per finalità promozionali di dati personali estratti dal database *della* mobile number portability

A seguito di numerose segnalazioni ricevute in merito ad sms promozionali che indicavano nel testo il gestore di appartenenza del ricevente, il Garante ha avviato un'istruttoria per verificare le modalità con cui era stato posto in essere tale trattamento.

Ne è emerso che la socierà che aveva curato la realizzazione della campagna promozionale si era avvalsa, essendo regolarmente iscritta al Registro operatori di comunicazione (Roc), del *database* della *mobile number portability* per individuare il gestore di appartenenza di ogni destinatario e personalizzare così maggiormente il messaggio promozionale. Il Garante pertanto ha dichiarato illecito tale trattamento in quanto le finalità di tale banca dati sono chiaramente definite dalla specifica disciplina dell'Agcom, che l'ha istituita, ed escludono espressamente l'utilizzo della stessa per finalità promozionali (provv. 23 luglio 2015, n. 436, doc. web n. 4260977).

11.7. *Le notificazioni di* data breach

Sono pervenute all'Autorità 49 comunicazioni di *data breach*, formulate dai più importanti fornitori di servizi di comunicazione elettronica operanti in Italia, registrando una crescita più che raddoppiata rispetto all'anno precedente.

La maggior parte delle violazioni notificate ha riguardato l'accesso non autorizzato ai dati personali o la perdita accidentale di documentazione contrattuale.

Inoltre, la quasi totalità dei casi notificati ha riguardato eventi che hanno coinvolto un numero di interessati inferiore a 100 essendosi verificati solo in 4 casi *data breach* di portata più ampia (oltre 2.000 soggetti coinvolti).

In tutti i casi sinora esaminati, l'Autorità, all'esito delle istruttorie svolte nei confronti dei fornitori, ha verificato che erano state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe assicurandosi, al contempo, che gli interessati erano stati informati dagli operatori nei casi previsti. Tuttavia, in un paio di casi si è reso necessario invitare gli operatori ad effettuare in maniera tempestiva la comunicazione agli interessati ritenendo che, contrariamente alle valutazioni fatte dall'operatore, ne ricorressero i presupposti (note 17 aprile e 22 dicembre 2015).

In quattro casi, è stato avviato un separato procedimento sanzionatorio per mancato rispetto dei termini previsti per la notificazione; in un caso infatti l'operatore aveva notificato l'evento al Garante e agli interessati con sei mesi di ritardo, mentre negli altri tre casi gli operatori non avevano effettuato alcuna comunicazione, ma il Garante è staro comunque informaro degli eventi attraverso segnalazioni pervenute da soggetti interessati dalle violazioni.

L'Autorità ha inoltre affrontato questioni di portata internazionale che in alcuni casi hanno avuto una vasta eco sui mezzi d'informazione (si veda, ad es., il caso Ashley Madison), interagendo con le competenti autorità estere per verificare l'eventuale e corretto trattamento dei dati personali di cittadini italiani.

Accanto alla gestione ordinaria delle comunicazioni di *data breach*, il Garante ha esaminato gli approfondimenti svolti in materia a livello europeo, partecipando ad una serie di incontri con le altre autorità competenti in ambito comunitario. I remi di maggiore rilievo hanno riguardato le modalità concrete da adottare in caso di violazioni di dati personali a carattere transnazionale e la valurazione delle misure tecnologiche di protezione adottate dai fornitori, con particolare riferimento all'inintelligibilità dei dati.

11.8. Data retention

È proseguira l'artività ispettiva avviata a partire dal 2012 in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico. Tali accertamenti sono volti a verificare il rispetto delle prescrizioni del Codice e del provvedimento generale del Garante in mareria di conservazione dei dati di traffico telefonico e telematico (provv. 17 gennaio 2008, doc. web n. 1482111, modificato dal provv. 24 luglio 2008, doc. web n. 1538224).

In diversi casi sono state accertate e contestate violazioni amministrative relativamente alla conservazione dei dati di traffico oltre i termini previsti e alla mancata adozione di alcune delle ulteriori misure di protezione prescritte dal cit. provvedimento del Garante, quali l'uso di tecnologie di riconoscimento biometrico per selezionare l'accesso alle aree e ai sisremi dove sono conservati i dati. In nessun caso, tuttavia, si è reso necessario adottare un provvedimento in quanto gli operatori hanno adottato tempestivamente idonee misure correttive.

11.9. *La geolocalizzazione di* smartphone *di persone disperse*

Il Garante ha dato parere favorevole all'uso di nuove tecnologie volte alla geolocalizzazione di persone disperse in montagna, capaci di rendere più rapide ed efficienti le operazioni di soccorso. I due nuovi sistemi, sottoposti al vaglio dell'Autorità dal Corpo nazionale soccorso alpino e speleologico (Cnsas), trasmetteranno i dati di