diritto alla protezione dei dati degli interessati e l'esigenza di informazione connessa al servizio di rilascio dei permessi di soggiorno (nota 16 marzo 2011).

Una comunità terapeutica aveva segnalato al Garante di aver ricevuto dalla locale questura la richiesta dell'elenco dei nominativi delle persone ricoverate presso la struttura. La questura ha chiarito all'Autorità che la richiesta era stata avanzata per dare seguito a un mandato di arresto dell'autorità giudiziaria nei confronti di un ospite della comunità. Il Garante ha ritenuto lecito il trattamento, tenuto conto delle specifiche esigenze di giustizia rappresentate (nota 14 luglio 2011).

Un Comando di polizia locale ha interpellato il Garante in ordine a un programma con il quale intendeva raccogliere, con l'autorizzazione verbale dei genitori, dati personali di minori (dati anagrafici; impronte digitali; caratteristiche fisiche particolari, quali cicatrici; patologie) e una ciocca dei loro capelli per un'eventuale analisi del Dna. I dati sarebbero stati riuniti in un Dvd da consegnare ai genitori, da utilizzare i dati in caso di rapimento, sparizione o per identificare cadaveri.

L'Autorità ha osservato che il programma prevedeva una raccolta di dati personali, anche sensibili e biometrici, effettuata in via preventiva, indiscriminata e massiva priva di riscontro nella normativa che disciplina i compiti affidati alle forze di polizia, sicché il progetto non poteva essere realizzato.

Richiesto di far conoscere le determinazioni adottate, il Comando ha comunicato di avere abbandonato il progetto (nota 22 giugno 2011).

6.2.1. Acquisizione di dati da parte delle forze di polizia

Nel 2011 il Ministero dell'interno ha sottoposto al Garante, per il parere "conforme", ossia obbligatorio e vincolante previsto dall'art. 54 del Codice, due convenzioni volte a disciplinare l'accesso delle forze di polizia a due importanti banche dati.

Il parere del Garante sulla convenzione tra la Direzione investigativa antimafia e l'Inail

Il primo parere era stato richiesto dal Dipartimento della pubblica sicurezza, Direzione investigativa antimafia (Dia) del Ministero, in ordine a uno schema di convenzione avente a oggetto l'accesso da parte della Dia alla banca dati detenuta dall'Inail relativa ai Documenti unici di regolarità contributiva (Durc), rilasciati dagli enti previdenziali, che attestano

contestualmente la regolarità –o meno– delle imprese in relazione agli adempimenti contributivi previdenziali, assistenziali e assicurativi posti dalla pertinente normativa. In particolare, il Durc costituisce condizione indispensabile per la partecipazione a gare d'appalto bandite da soggetti pubblici.

L'accesso da parte della Dia alla banca dati gestita dell'Inail, è risultato pertinente all'attività di monitoraggio degli appalti pubblici istituzionalmente affidata alla Direzione in base alle vigenti disposizioni (art. 15, d.lgs. 20 agosto 2002, n. 190, confermato dall'art. 180 del d.lgs. 12 aprile 2006, n. 163, cd. *"Codice degli appalti"*; decreto del Ministero dell'interno del 14 marzo 2003).

Le clausole della convenzione sono state stabilite attraverso incontri tecnici e approfondimenti svolti dall'Autorità con le parti, che hanno fornito piena collaborazione.

In particolare:

- l'accesso, per la sola consultazione, della Dia alla banca dati è espressamente limitato al monitoraggio degli appalti pubblici; sono abilitati all'accesso solo gli utenti cui sono attribuite dalla Dia stessa specifiche credenziali di abilitazione personali;
- la Dia deve impartire al personale abilitato le istruzioni relative alle responsabilità connesse all'accesso improprio alla banca dati, all'uso illegittimo delle informazioni e alla loro indebita divulgazione, comunicazione e cessione a terzi, ed entrambe le parti hanno l'obbligo di formazione di detto personale all'utilizzo della banca dati;
- la comunicazione tra i sistemi informativi della Dia e dell'Inail avviene attraverso la rete del sistema pubblico di connettività *Spc/Infranet VPN*, che opera cifrando la comunicazione dalla sorgente alla destinazione e garantisce l'identità delle parti comunicanti;
- l'Inail provvede al tracciamento degli accessi, che consente di verificare anche le operazioni eseguite da ciascun utente e mette a disposizione della Dia una reportistica periodica relativa agli accessi effettuati dagli utenti e alle operazioni svolte, nonché all'introduzione nel sistema di specifici sistemi (*alert*) volti a segnalare in tempo reale alla Dia stessa accessi anomali rispetto a parametri predeterminati;
- la convenzione indica la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni al testo di essa.

Poiché tali modalità di collegamento fra i sistemi informatici e di accesso delle forze di polizia alla banca di dati Durc sono conformi alla disciplina in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza, il Garante ha espresso parere favorevole sulla convenzione (parere 14 aprile 2011 [doc. *web* n. 1813942]).

Il parere del Garante sulla convenzione tra il Ministero dell'interno e l'Agenzia delle entrate

La seconda richiesta di parere ha riguardato la convenzione avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (CED) del predetto Dipartimento della pubblica sicurezza, alla banca dati dell'Anagrafe tributaria, detenuta dall'Agenzia delle entrate, attraverso l'applicativo informatico denominato Puntofisco.

La richiesta è risultata fondata sulla l. 31 maggio 1965, n. 575, che prevede tra l'altro, da parte dei questori, sia l'adozione di misure di prevenzione nei confronti degli indiziati di appartenere alla criminalità organizzata, sia, anche a mezzo della Guardia di finanza o della polizia giudiziaria, che agisce anche ai sensi dell'art. 55 c.p.p., lo svolgimento di indagini sul tenore di vita, sulle disponibilità finanziarie e sul patrimonio di tali soggetti e di alcuni familiari.

A tali fini il questore può richiedere ad ogni ufficio della pubblica amministrazione, ad ogni ente creditizio nonché alle imprese, società ed enti di ogni tipo, informazioni e copia della documentazione ritenuta utile.

Anche in questo caso il testo della convenzione è stato oggetto di modifiche attraverso incontri tecnici e approfondimenti svolti dall'Autorità con le parti, che hanno fornito piena collaborazione. In particolare:

- costituiscono oggetto della convenzione i soli dati anagrafici, reddituali e fiscali dei soggetti censiti nell'anagrafe tributaria, non i dati sensibili;
- l'accesso delle forze di polizia alla banca dati, per la sola consultazione, è espressamente limitato alle finalità connesse allo svolgimento delle attività previste dalla normativa sopra indicata (l. n. 575/1965 e art. 55 c.p.p.), nei limiti da questa posti;
- possono accedere alla banca dati gli operatori delle forze di polizia con qualifica di ufficiale o agente di polizia giudiziaria cui sono attribuiti dal CED specifici profili di abilitazione e credenziali di autenticazione personali;
- il CED deve impartire al personale abilitato direttive relative alle responsabilità connesse all'accesso improprio alla banca dati, all'uso illegittimo delle informazioni e alla loro

indebita divulgazione, comunicazione e cessione a terzi, ed è, altresì, previsto per entrambe le parti l'obbligo di formazione di detto personale all'utilizzo della banca dati;

- sono stati previsti specifici divieti a carico del CED, e il correlativo obbligo per il centro di impartire direttive agli utenti, in materia di duplicazione delle informazioni acquisite per la creazione di autonome banche dati e di utilizzo di dispositivi automatici (robot) che consentono la consultazione in forma massiva dei dati personali;
- per quanto concerne la sicurezza nel flusso dei dati è previsto l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia dei dati trasferiti da *client* e *server*;
- il CED provvede al tracciamento degli accessi alla banca dati e l'Agenzia provvede al tracciamento anche dell'accesso ai dati ivi detenuti;
- il testo indica la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla convenzione.

L'Autorità ha, peraltro, ritenuto che la convenzione dovesse essere ulteriormente integrata con alcune disposizioni relative, in particolare:

- all'inclusione dell'applicativo Puntofisco tra quelli sottoposti ai sistemi del CED relativi al monitoraggio degli accessi e agli alert su anomalia;
- al riferimento alla disponibilità per i capi degli uffici dei risultati di tale attività di monitoraggio e alert per almeno trenta giorni nel portale del CED;
- all'obbligo per quest'ultimo di fornire istruzioni preventive e vincolanti ai capi degli uffici sulla verifica puntuale e tempestiva degli alert;
- all'obbligo per l'Agenzia di fornire al Ministero strumenti idonei a consentire il monitoraggio delle operazioni compiute e a supportare i controlli, anche a campione, sulle attività svolte dagli utenti.

A condizione che il testo venisse in tal modo integrato, il Garante ha quindi espresso parere favorevole sulla convenzione (parere 26 maggio 2011 [doc. *web* n. 1822278]).

6.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

Si è riferito nella Relazione 2010, p. 96, della richiesta del Garante al Ministero dell'interno - Dipartimento di pubblica sicurezza, di indicare con precisione i tempi per la realizzazione

delle misure prescritte dall'Autorità per rafforzare la sicurezza nel trattamento dei dati effettuato per l'attuazione della Convenzione di Schengen.

Alla luce delle indicazioni ricevute e delle difficoltà rappresentate dal Ministero, il Garante con provvedimento del 31 marzo 2011 ha disposto il differimento dei termini per l'adempimento delle prescrizioni, che sono in corso di attuazione.

Accesso diretto

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nella sezione nazionale del SIS (cd. "N-SIS"), in virtù delle quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per tale sezione, ossia al Dipartimento della pubblica sicurezza (cd. "accesso diretto"). Il numero e il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante non hanno subito sostanziali variazioni rispetto all'anno precedente.

Anche nel 2011 sono aumentate le richieste di accesso ai dati pervenute al Garante da autorità di controllo di sezioni nazionali del SIS di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni degli artt. 109 e 114 della convenzione.

7. ATTIVITÀ GIORNALISTICA

7.1. MINORI

Il Garante si è occupato nuovamente del delicato rapporto tra libertà di informazione e tutela della riservatezza dei minori, quali soggetti particolarmente vulnerabili in caso di esposizione mediatica.

Meritevole di citazione è l'intervento relativo alla diffusione delle notizie concernenti la nascita di due gemelle siamesi, volto ad assicurare il rigoroso rispetto delle garanzie poste a tutela dei minori dal codice deontologico per l'attività giornalistica e dalla Carta di Treviso. Questo perché, in particolare, erano stati riportati i nomi delle bambine unitamente a taluni dettagli relativi al loro stato fisico e di salute al momento della nascita, agli interventi chirurgici subìti, nonché alle complesse e dolorose decisioni che i genitori sono stati chiamati ad assumere riguardo agli interventi futuri e alle relative conseguenze sulla vita delle neonate (comunicato stampa 25 luglio 2011 [doc. *web* n. 1826445]).

Il Garante, inoltre, è intervenuto per arginare l'eccessiva spettacolarizzazione di eventi di cronaca relativi a minori, come ad esempio nel caso della giovane ragazza ritrovata morta a Tradate, per il quale ha emanato un apposito comunicato stampa il 2 aprile 2011 [doc. *web* n. 1802262].

7.1.1. Vittime di abusi

In due casi nei quali alcuni quotidiani, nel riferire dell'avvio di un'indagine su presunti abusi sessuali ai danni di una minorenne, avevano diffuso dati ritenuti idonei ad identificarla indirettamente, l'Autorità ha ribadito che non si possono pubblicare dettagli che rendono identificabili vittime di violenza sessuale, tanto più se si tratta di minori. Pertanto, anche i nomi dei violentatori non possono essere diffusi se rendono identificabile la vittima. 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 riguardino

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 (comunicati stampa 16 luglio [doc. *web* n.1823757] e 4 agosto 2011 [doc. *web* n. 1828618]).

7.2. CRONACHE GIUDIZIARIE E VITTIME DI REATO

L'Autorità ha risposto a diversi reclami e segnalazioni richiamando il principio, ormai consolidato, secondo cui 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.).

Il richiamato parametro dell'essenzialità dell'informazione ha costituito criterio per valutare diversi trattamenti di dati i quali, pur se attinenti a fatti giudiziari di rilevante interesse pubblico, includevano riferimenti a soggetti terzi la cui identità era meritevole di tutela (ad esempio familiari, anche minorenni, di persone interessate da procedimenti penali, parti lese, ecc.), oppure a elementi che, pur essendo relativi alle persone indagate, risultavano eccedenti rispetto alle finalità informative, come l'indicazione della via e del numero civico dell'abitazione in cui si era verificato un furto (nota 20 giugno 2011).

7.2.1. Truffa dei Parioli

Anche a seguito della segnalazione di un'associazione di consumatori, sul noto caso della pubblicazione sulla stampa di ampi elenchi di risparmiatori vittime di una truffa messa in atto da una società finanziaria, il Garante ha invitato a non proseguire la pubblicazione indiscriminata di dati personali riferibili alle vittime stesse.

Gli elenchi pubblicati contenevano, infatti, nominativi di centinaia di cittadini, da considerarsi allo stato vittime di reato, i cui dati personali venivano così divulgati in maniera indiscriminata.

L'Autorità ha precisato che, prima di diffondere tali nominativi, è necessario valutare di volta in volta la sussistenza di alcuni precisi presupposti, in particolare se si tratti di persone non note, che non abbiano rilasciato dichiarazioni alla stampa, se le loro vicende personali non siano prive di specifico rilievo in ragione della somma investita e se nei loro confronti siano stati avviati specifici accertamenti o formulate formali contestazioni (nota 28 aprile 2011 e comunicato stampa 5 aprile 2011 [doc. *web* n. 1802648]).

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

Nel 2011 sono pervenute segnalazioni e reclami sulla diffusione di dati personali di personaggi pubblici o persone che esercitano pubbliche funzioni.

Il Garante ha ribadito che sussistono margini più ampi nella diffusione di informazioni relative a tali persone, che possono riguardare, entro certi limiti, anche notizie attinenti alla vita privata. In tal senso, in un caso di diffusione, da parte di un quotidiano, di dati relativi al ricovero in ospedale di un consigliere regionale, l'Autorità ha ritenuto che la particolare dinamica dei fatti narrati e il contesto nei quali si sarebbero svolti potessero giustificare la narrazione della vicenda, essendo stato riportato che lo stesso interessato si sarebbe affacciato ad un balcone nel corso dell'episodio narrato ed essendo stato rappresentato –nell'istruttoria amministrativa aperta sul caso dall'Ufficio del Garante– che notizie sull'interessato erano state richieste all'ospedale ancor prima del suo arrivo (nota 20 aprile 2011).

7.3.1. Diffusione di un documentario su una raffineria sarda

In un reclamo concernente un film documentario sull'impatto di una raffineria sarda sulla popolazione e sull'ambiente circostante, veniva contestata la legittimità di alcune interviste riportate nel documentario stesso e la impossibilità di poter replicare alle tesi ivi sostenute.

Il Garante in questo caso ha evidenziato che i dirigenti della raffineria avevano rilasciato le interviste volontariamente a un giornalista che aveva preliminarmente reso nota la propria identità, e che i temi affrontati nel film documentario erano da ritenersi di pubblico interesse e affrontati in termini essenziali. Pertanto, non ha ravvisato gli estremi per adottare provvedimenti inibitori (nota 22 dicembre 2011).

7.4. 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).

In relazione alla pubblicazione da parte di agenzie di stampa e quotidiani –anche *online*– del nome, dell'iniziale del cognome e dell'età di una infermiera in servizio presso il reparto di neonatologia di un ospedale, risultata positiva ai *test* sulla tubercolosi, l'Autorità ha ricordato che i mezzi di informazione sono tenuti a valutare con scrupolo l'interesse pubblico delle singole informazioni diffuse e pertanto i *media* devono evitare di riportare informazioni non essenziali che possano ledere la riservatezza delle persone coinvolte (comunicato stampa 24 agosto 2011 [doc. *web* n. 1832410]).

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, in particolare nei casi di suicidio (nota 22 settembre 2011).

7.5. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

Anche nel 2011 il Garante ha ricevuto diverse segnalazioni e ricorsi concernenti la reperibilità dei dati personali a distanza di anni, in quanto rinvenibili negli archivi storici dei giornali *online* (v. in argomento anche il par. 15.6.).

L'Autorità, al riguardo, ha ribadito che la diffusione sui siti internet di quotidiani *online* di articoli contenenti informazioni su fatti anche molto delicati e piuttosto risalenti nel tempo, in quanto riconducibile all'archivio storico della testata non integra, in linea di principio, un illecito trattamento di dati personali (v. Relazione 2010, p. 105).

È stato pertanto dichiarato infondato un ricorso volto ad ottenere l'aggiornamento delle notizie giudiziarie riportate negli archivi storici *online*, o comunque l'oscuramento dei dati del ricorrente o l'uso di iniziali in luogo del nome, poiché l'Autorità ha rilevato che il

trattamento effettuato per fini storici, per espressa previsione normativa (art. 99, comma 1, del Codice), è considerato compatibile con i diversi scopi per i quali i dati erano stati in precedenza raccolti o trattati, sicché deve ritenersi lecito (provv. 8 marzo 2012 [doc. *web* n. 1887094]).

Tuttavia, in alcuni casi 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 potesse comportare un sacrificio sproporzionato dei suoi diritti.

L'Autorità, in tali casi ha richiesto pertanto che la pagina *web* contenente i dati personali dell'interessato (quale è, anzitutto, il suo nominativo) fosse sottratta alla diretta individuabilità tramite i comuni motori di ricerca, pur restando inalterata nel contesto dell'archivio e consultabile telematicamente accedendo all'indirizzo *web* dell'editore (v. tra gli altri, provv.ti 23 marzo 2011 [doc. *web* n. 1807050] e 21 dicembre 2011 [doc. *web* n. 1877115]). Sull'argomento si segnala una sentenza del Tribunale di Roma del 28 novembre 2011, riguardante il trattamento dei dati personali contenuti in una interrogazione parlamentare del Senato, diffusa sul *web*, contenente notizie non attuali e non contestualizzate. Il Tribunale ha ordinato all'amministrazione del Senato di rendere tecnicamente non possibile la diretta individuazione, tramite i comuni motori di ricerca, della pagina *web* relativa all'atto di sindacato ispettivo.

L'interessato si era rivolto al Tribunale avverso l'inammissibilità, dichiarata dal Garante, del suo ricorso riguardante la vicenda. Tale decisione era stata motivata rilevando che il trattamento risultava effettuato dal Senato in relazione a un atto di sindacato ispettivo nell'esercizio di funzioni e prerogative parlamentari, in ossequio al principio di pubblicità degli atti parlamentari, e dunque nell'ambito della sfera di autonomia costituzionalmente riservata (art. 64, comma 2, Cost.). Nella decisione l'Autorità aveva peraltro ribadito che, nel caso di pubblicazione *online* di interrogazioni spesso recanti minute ricostruzioni di fatti poi rivelatisi non veri, la soluzione migliore poteva essere inibire l'accesso da parte dei motori di ricerca generalisti agli atti di sindacato ispettivo [doc. *web* n. 1638472].

7.6. RINTRACCIABILITÀ SUL MOTORE DI RICERCA *GOOGLE* E DIRITTO ALL'OBLIO

Talvolta, nonostante l'invito rivolto dal Garante al titolare del trattamento a rendere non indicizzabile dall'esterno, mediante i comuni motori di ricerca, un determinato articolo giornalistico, è stato segnalato dall'interessato che esso restava rinvenibile mediante il motore di ricerca di *Google*, benché l'editore avesse dichiarato di aver attivato la procedura a tal fine prevista dallo stesso motore di ricerca.

In particolare, in un caso è stata coinvolta direttamente *Google Italy S.r.l.* per un approfondimento della questione, soprattutto dal punto di vista tecnico.

Dall'istruttoria preliminare è emerso che la persistente rintracciabilità di articoli mediante i comuni motori di ricerca è dovuta sia alla circostanza che talora l'articolo –inserito nell'archivio storico *online* di una determinata testata o sito *web*– è stato ripreso anche da altri siti, *forum* o blog, o comunque residua sul *web* come copia *cache*, non ancora eliminata dal *crawler* di *Google*, sia alla complessità della procedura necessaria per conseguirne la effettiva non indicizzabilità.

Infatti, tale procedura si compone di tre fasi, fra loro sostanzialmente complementari: la compilazione del *file robot txt*, finalizzato a inibire l'accesso ai file e alle *directory* propria del *server* del sito ove è pubblicato l'articolo; lo strumento del *metatag noindex*, avente scopo di impedire che i contenuti di esso vengano elencati nell'indice di *Google* qualora altri siti –diversi da quello relativo alla testata che ha pubblicato l'articolo– contengano link alla medesima pagina; lo strumento di rimozione degli *URL*, finalizzato a "nascondere" con urgenza– in attesa del passaggio del *crawler* e quindi della definitiva deindicizzazione– l'articolo in questione dai risultati di ricerca per impedire che siano mostrati risultati relativi ad una pagina *web* completamente rimossa.

L'editore titolare del trattamento è stato quindi invitato dall'Autorità a porre in essere tale procedura e, ottenuta in questo modo la deindicizzazione, l'Autorità stessa ha deciso di non adottare provvedimenti prescrittivi (note 1° giugno e 1° agosto 2011).

8. TRATTAMENTO DI DATI PERSONALI ATTRAVERSO INTERNET

Il crescente utilizzo della rete nello svolgimento delle relazioni economiche e delle attività sociali ha evidenziato anche quest'anno diverse problematiche relative al trattamento dei dati.

8.1. TRATTAMENTO DATI *ONLINE* DA PARTE DI COMPAGNIE AEREE E SITI DI PRENOTAZIONE DI VIAGGI E ALBERGHI

Nel 2011 è stata avviata un'istruttoria preliminare sul trattamento di dati da parte di una nota società specializzata nella prenotazione *online* di viaggi e alberghi, che, nel richiedere la registrazione al proprio sito, in qualità di soggetto intermediario, prevedeva l'inserimento obbligatorio di alcuni dati personali dell'utente, quali il tipo e il numero del documento d'identità.

Al riguardo l'Ufficio ha richiesto informazioni alla società, per verificare in particolare il rispetto dei princìpi di proporzionalità e non eccedenza del trattamento rispetto alle finalità perseguite, *ex* art. 11 del Codice (nota 20 giugno 2011).

La società ha risposto di aver chiesto alla sua sede centrale di eliminare dai campi obbligatori la voce relativa al documento d'identità.

In un altro caso, il trattamento dei dati personali (e in particolare degli estremi dei documenti d'identità) dei passeggeri, nell'ambito del servizio di *check-in online* effettuato da una nota compagnia aerea *low-cost* –in qualità di vettore erogatore diretto del servizio di trasporto aereo e non di mero intermediario nella ricerca e prenotazione dei voli disponibili– non è risultato in contrasto con i suindicati princìpi di proporzionalità e non eccedenza del trattamento dati sanciti dall'art. 11 del Codice.

Infatti, gli estremi del documento d'identità sono stati ritenuti funzionali alle finalità di elaborazione della prenotazione e di sicurezza, espressamente dichiarate nell'informativa *ex* art. 13 del Codice, rilasciata dalla società al momento del *check-in*.

8.2. RICEVITORIE E TABACCHERIE: GARANZIE PER LA RACCOLTA E IL TRATTAMENTO DEI DATI

L'Autorità ha svolto, a partire dal mese di ottobre 2011, un ciclo di accertamenti ispettivi per verificare il rispetto della normativa in materia di protezione dei dati personali, nell'ambito

dei giochi e servizi disponibili presso ricevitorie e punti vendita, quali, ad esempio, ricariche telefoniche e di tv digitale, rilascio di carte telefoniche e pagamento bollette.

In particolare, l'Autorità con provvedimento del 15 dicembre 2011 [doc. *web* n. 1883880], ha ribadito che la capacità di autodeterminazione dell'interessato non è assicurata quando si assoggetta l'accesso a un servizio –qual è l'abilitazione delle ricevitorie ai giochi e servizi forniti da una primaria società– alla preventiva autorizzazione a trattare per una diversa finalità, come quella pubblicitaria o quella di comunicazione a soggetti terzi, i dati conferiti per il servizio medesimo (cfr.: provv. 12 ottobre 2005 [doc. *web* n. 1179604]; provv. 3 novembre 2005 [doc. *web* n. 1195215]; provv. 10 maggio 2006 [doc. *web* n. 1298709]; provv. 22 febbraio 2007 [doc. *web* n. 1388590]).

È stato pertanto inibito alla società in questione il trattamento dei dati delle ricevitorie (che non siano persone giuridiche, associazioni o enti, in buona misura esclusi dall'ambito di applicazione del Codice ad opera del d.l. n. 201/2011, convertito con modificazioni dalla l. n. 214/2011, come più diffusamente indicato al par. 2.1.1.) erogatrici di giochi e/o servizi della medesima, acquisiti tramite la domanda di abilitazione presente sul sito della società, per l'invio di comunicazioni promozionali relative a giochi e/o servizi diversi da quelli contrattualizzati con le ricevitorie stesse, e per la comunicazione di dati a soggetti terzi, senza aver ottenuto un consenso libero, specifico, espresso e documentato per iscritto, *ex* art. 23 del Codice, per ciascuna delle predette finalità. È stato inoltre prescritto alla medesima società di modificare i moduli di raccolta dati *online*, prevedendo la richiesta di un consenso specifico per ciascun trattamento dati effettuato.

8.3. IL TRATTAMENTO DATI REALIZZATO DALLE UNIVERSITÀ TELEMATICHE ED ENTI DI FORMAZIONE

Nel 2011 è stato analizzato dall'Autorità, il trattamento dati effettuato da varie università telematiche ed enti di formazione, operanti su tutto il territorio nazionale, anche sulla base di ispezioni mirate del Nucleo speciale *privacy* della Guardia di finanza (sulla cui attività v. più in dettaglio par. 17.2.).

Dalle ispezioni è emerso che in più casi i form di registrazione ai siti *web* prevedevano l'acquisizione di un unico consenso per diverse finalità di trattamento dati. Talora, già dopo

l'ispezione oppure dopo la richiesta di informazioni rivolta dall'Autorità, le società titolari del trattamento hanno modificato la configurazione delle modalità di acquisizione del consenso, inserendo la richiesta di un consenso specifico per ciascun trattamento dati effettuato.

Più in dettaglio, il provvedimento 19 ottobre 2011 [doc. *web* n. 1844176] ha stabilito che, attraverso il form di iscrizione ad un sito *web*, si possono raccogliere solo i dati personali strettamente necessari a fornire il servizio per il quale l'utente si registra, vietando ad una università telematica il trattamento di alcuni dati degli studenti che si erano iscritti *online* per essere informati sulle attività dell'ateneo.

Nel corso di accertamenti ispettivi era emerso infatti che l'università, mediante il form di registrazione al sito, raccoglieva anche informazioni, quali luogo e data di nascita, codice fiscale, cittadinanza, eccedenti rispetto alle finalità dichiarate di mantenere contatti con gli utenti interessati al mondo dell'ateneo e di informare sulle novità e gli appuntamenti universitari.

Oltre al divieto, l'Autorità ha prescritto all'ateneo di modificare le modalità di raccolta *online* dei dati personali, eliminando dal form di registrazione la richiesta dei dati risultati non pertinenti e nel caso in cui intenda comunicare i dati personali a terzi, di indicare chiaramente nell'informativa i soggetti o le categorie di soggetti, i motivi della comunicazione, acquisendo il consenso degli utenti.

8.4. TRATTAMENTO DI DATI SANITARI SU *FORUM* E BLOG

Dopo una complessa istruttoria, avviata nel 2010, a inizio 2012 il Garante ha varato importanti ed innovative linee-guida (provv. 25 gennaio 2012, in G.U. 20 febbraio 2012, n. 42 [doc. *web* n. 1870229]) per i siti *web* dedicati alla salute (che non riguardano comunque i servizi di assistenza sanitaria *online* e la telemedicina), per accrescere il livello di tutela di chi è iscritto a *social network* dedicati alla salute, partecipa a blog e a *forum* di discussione o segue siti *web* che si occupano esclusivamente di tematiche sanitarie.

In sintesi, ai gestori di tali siti, blog, *forum*, e *social network*, si raccomanda di avvertire gli utenti dei potenziali rischi connessi alla pubblicazione e alla diffusione *online* dei dati relativi alla loro salute, in particolare, inserendo in home page un'apposita "avvertenza di rischio". Ciò con lo scopo di "mettere in guardia" l'utente sulla possibilità che i suoi "messaggi" lo

rendano identificabile in relazione alla propria patologia, e che le informazioni inserite possano essere indicizzate dai motori di ricerca generalisti o conosciute dalla generalità degli utenti internet e non dai soli utenti iscritti ad uno specifico sito.

In tal modo è data all'utente, informato del rischio in questione (e al quale è chiesto di dare conferma di aver preso visione dell'avviso di rischio, barrando un'apposita casella) la possibilità di decidere consapevolmente se inserire o meno dati personali (es. nome, cognome, e-mail ecc.) che possano rivelare, anche indirettamente, l'identità propria o di terzi, così come pure se pubblicare foto o video che consentano di rendere identificabili persone e luoghi.

I *forum* e/o blog che prevedono la registrazione sono tenuti anche ad informare gli utenti sugli scopi per i quali i dati sono richiesti, sulle modalità del loro trattamento, sui tempi di conservazione, sul diritto di cancellare, aggiornare, rettificare o integrare i dati così raccolti, come previsto dal Codice.

Il Garante ha infine stabilito che i dati raccolti dai gestori dei siti devono essere protetti da rigorose misure di sicurezza, restare riservati e non essere comunicati o diffusi a terzi, e che il relativo trattamento sia effettuato solo da personale autorizzato.

8.5. I SERVIZI OFFERTI DA MOTORI DI RICERCA

Google Analytics e *Google* Gruppi

Nel 2011 il Garante ha analizzato alcuni profili del servizio fornito da *Google Analytics* con riguardo alla protezione dei dati personali degli utenti.

In particolare l'indagine, condotta all'interno del sotto-gruppo *"technology"* del Gruppo Art. 29, ha evidenziato alcune carenze del suddetto servizio sia con riferimento all'informativa rilasciata da *Google* ai gestori di siti *web*, sia con riferimento alle procedure poste in essere per consentire agli utenti l'esercizio del diritto di opposizione alla raccolta dei relativi dati di navigazione, utilizzati per le analisi di traffico condotte dal *webmaster*.

Il contributo del Garante si è rivelato prezioso anche in considerazione dell'attività istruttoria avviata dall'Autorità tedesca di protezione dei dati del Land di Amburgo a seguito della quale è stato adottato un documento ufficiale contenente linee-guida di carattere operativo per un uso del servizio *Google Analytics* da parte dei *webmaster*, in linea con la normativa europea sulla protezione dei dati.

Google Analytics si è impegnata a rispettare le menzionate linee-guida nei confronti di tutti i *webmaster* operanti nell'Ue. Tali assicurazioni sono state trasmesse, da parte dell'Autorità tedesca del Land di Berlino (che coordina l'attività dell'"International Working Group on Data Protection in Telecommunications" - Gruppo di Berlino), a tutte le Autorità europee di protezione dei dati.

I punti essenziali del predetto documento, concordati in sede europea, hanno previsto: 1) una migliore definizione dei ruoli dei soggetti coinvolti, ovvero di *Google* in qualità di *processor* e del *webmaster* in qualità di *controller*; 2) lo sviluppo di strumenti che consentano ai *webmaster* di indirizzare a *Google* istruzioni precise e dettagliate che permettano un corretto trattamento dei dati di navigazione sulla base delle reali necessità del *controller*; 3) la previsione di agevoli meccanismi di opposizione da parte degli utenti alla raccolta dei propri dati di navigazione; 4) la previsione di strumenti di anonimizzazione degli indirizzi IP; 5) la definizione di una corretta *policy* di *data retention*.

Il Garante è intervenuto anche nei confronti del servizio *Google* Gruppi, a seguito di alcune segnalazioni che riguardavano la diffusione di dati personali contenuti in alcuni *post* presenti in *newsgroup*, indicizzati dalla piattaforma *Google* Gruppi. In particolare l'Autorità, dopo una lunga ed articolata istruttoria, ha richiesto, per il tramite di *Google Italy S.r.l.*, che *Google Inc.* (proprietaria e gestore del servizio *Google* Gruppi) intervenisse sul trattamento dei dati personali degli utenti, presenti nei *newsgroup* indicizzati dal servizio, nei casi in cui il relativo trattamento risultasse eccedente e non pertinente rispetto alle finalità proprie di un gruppo di discussione sulla rete *web*, attraverso la rimozione dei post che contenevano dati personali non necessari.

L'Autorità ha ottenuto tale intervento nonostante la società, come risulta anche dall'informativa fornita agli utenti, abbia sede fuori dal territorio italiano.

Il particolare caso di *Google Suggest*: l'associazione automatica di termini

In una segnalazione è stato lamentato che il servizio *Google Suggest* associava al nome del segnalante il termine "mafia".

Il Garante, rilevato che tale servizio collega alle parole chiave digitate dagli utenti una serie di "suggerimenti di ricerca", ossia potenziali termini, presumibilmente affini, che iniziano con le prime lettere o parole già digitate dall'utente, così esonerandolo dal dover digitare il testo