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

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

8.6. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

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

Giornali *online*

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

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

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

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

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

Informazioni *online*

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

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

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

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

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

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

9.1. Diffusione di dati sensibili su Internet

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

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

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

9.2. *Forum* e *blog*

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

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

Libera manifestazione del pensiero

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

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

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

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

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

Dati sanitari

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

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

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

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

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

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

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

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

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

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

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

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

9.3. *FACEBOOK*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Raccolta del consenso per diverse finalità e modalità del trattamento

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

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

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

Il Registro delle opposizioni

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

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

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

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

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

Modelli di informativa resa agli abbonati dagli operatori telefonici

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

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

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