GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Protezione dei dati, trasparenza e tecnologie della comunicazione

Relazione 2012

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it

Protezione dei dati, trasparenza e tecnologie della comunicazione

Relazione 2012

www.garanteprivacy.it

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

II. ATTIVITÀ SVOLTA DAL GARANTE

INDICE

INDICE

III. L'UFFICIO DEL GARANTE

IV. DOCUMENTAZIONE

Elenco delle abbreviazioni

La presente Relazione è riferita al 2012 e contiene talune notizie già anticipate nella precedente edizione, nonché alcune ulteriori informazioni, aggiornate al 31 gennaio 2013, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	*ad esempio*
art.	*articolo*
c.c.	*codice civile*
c.p.	*codice penale*
c.p.c.	*codice di procedura civile*
c.p.p.	*codice di procedura penale*
cd.	*cosiddetto/a*
cfr.	*confronta*
Codice	*Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)*
Cost.	*Costituzione*
d.l.	*decreto-legge*
d.lgs.	*decreto legislativo*
d.m.	*decreto ministeriale*
d.P.C.m.	*decreto del Presidente del Consiglio dei ministri*
d.P.R.	*decreto del Presidente della Repubblica*
G.U.	*Gazzetta Ufficiale della Repubblica italiana*
G.U.U.E.	*Gazzetta Ufficiale dell'Unione europea*
l.	*legge*
lett.	*lettera*
n.	*numero*
p.	*pagina*
p.a.	*pubblica amministrazione*
pp.aa.	*pubbliche amministrazioni*
par.	*paragrafo*
provv.	*provvedimento del Garante per la protezione dei dati personali*
Relazione	*Relazione annuale del Garante*
r.d.	*regio decreto*
reg.	*regolamento*
t.u.	*testo unico*
UE	*Unione europea*
v.	*vedi*

Stato di attuazione del Codice in materia di protezione dei dati personali

I. Stato di attuazione del Codice in materia di protezione dei dati personali

1. Sintesi di alcuni provvedimenti e attività istituzionali di particolare rilievo

Da uno sguardo d'insieme ai provvedimenti più significativi del periodo al quale questa Relazione si riferisce, di seguito sommariamente illustrati, emerge la varietà degli ambiti nei quali si sono posti problemi di protezione dati.

La complessità delle decisioni adottate ha riguardato tanto profili specificatamente giuridici, anche in relazione alla evoluzione del contesto normativo ed alle novità intervenute in materia di protezione dati, quanto tecnico-informatici.

1.1. Giustizia e pubblica sicurezza

In materia di giustizia e ordine pubblico alcune deliberazioni collegiali si segnalano per il loro rilievo generale.

Consultazione Sistema informativo Casellario

Su richiesta del Ministero della giustizia, il Garante ha espresso parere favorevole sullo schema di decreto dirigenziale riguardante la consultazione diretta, per via telematica, del Sistema informativo del Casellario (SiC) da parte delle amministrazioni pubbliche, dei gestori di pubblici servizi e dell'autorità giudiziaria (ai sensi dell'art. 39 d.P.R. 14 novembre 2002, n. 313, t.u. delle disposizioni in materia di Casellario giudiziario).

Il testo esaminato è volto, in particolare, ad assicurare un accesso selettivo ai soli dati giudiziari indispensabili per lo svolgimento degli accertamenti di competenza, tramite l'introduzione dell'apposito "certificato selettivo", per evitare che al soggetto richiedente siano rese disponibili, temporaneamente, anche eventuali iscrizioni di provvedimenti giudiziari non strettamente correlati agli accertamenti in corso (provv. 11 ottobre 2012 [doc. web n. 2091248]).

Permesso di soggiorno elettronico

Di significativa rilevanza anche il parere favorevole allo schema di decreto interministeriale che adegua il permesso di soggiorno rilasciato a cittadini di Paesi terzi al modello uniforme adottato dagli altri Stati comunitari. In base al nuovo decreto chi ottiene il permesso sarà fornito di una tessera, dotata di un microprocessore -contenente sia le informazioni necessarie a verificare l'autenticità del documento, sia i dati identificativi, la fotografia e le impronte digitali del titolare- che potrà essere letto esclusivamente dagli organi di controllo. I dati del cittadino straniero saranno registrati in un archivio elettronico presso il Centro elettronico nazionale (Cen) della polizia di Stato, conservati per i periodi puntualmente indicati nel decreto e potranno essere utilizzati solo per finalità relative alla verifica e alla gestione del permesso di soggiorno.

Nell'esprimere il parere l'Autorità si è riservata di valutare le regole tecniche con le quali saranno precisate le misure da adottare per garantire la riservatezza, l'integrità e la sicurezza dei dati trattati (provv. 5 giugno 2012 [doc. web n. 1908393]).

Il Garante ha altresì formulato il suo parere ai sensi dell'art. 54 del Codice, su due convenzioni relative all'accesso delle forze di polizia, tramite il Ced -Ministero dell'interno, a grandi banche dati.

Il parere sulla Convenzione tra il Ministero dell'interno e l'Inps

Il primo parere ha riguardato l'accesso alla banca dati dell'Inps, per l'adozione di misure di prevenzione e lo svolgimento di indagini sul tenore di vita e le disponibilità finanziarie degli indiziati di appartenere alla criminalità organizzata (l. 31 maggio 1965, n. 575) (provv. 2 febbraio 2012 [doc. web n. 1875293]).

La Convenzione in parola definisce in particolare la tipologia dei dati oggetto dell'accesso (dati anagrafici, retributivi, contributivi e pensionistici dei soggetti censiti dall'Inps), le finalità dell'accesso (esclusivamente quelle connesse allo svolgimento delle attività previste dalla suddetta normativa) ed il personale ad esso abilitato (operatori delle forze di polizia con qualifica di ufficiale o agente di polizia giudiziaria).

Al Ced è esplicitamente vietato duplicare le informazioni per creare banche dati autonome, nonché utilizzare dispositivi automatici che consentono la consultazione in forma massiva dei dati personali. Per quanto concerne la sicurezza, è previsto l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia nel flusso dei dati. Inoltre, il Ced monitora gli accessi alla banca dati e rileva eventuali anomalie.

L'Autorità ha subordinato il proprio parere favorevole in particolare, all'indicazione che l'Allegato B della Convenzione, contenente l'analitica indicazione dei dati consultabili, costituisce parte integrante della medesima (parere 2 febbraio 2012 [doc. web n.1875293]).

Il parere sulla Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze

Il secondo parere ha riguardato l'accesso ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf) gestito dal Ministero dell'economia e delle finanze (l. 17 agosto 2005, n. 166 e d.m. del Ministero dell'economia e delle finanze 30 aprile 2007, n. 112) (provv. 12 luglio 2012 [doc. web n. 1915461]).

Anche in questo caso il testo della Convenzione individua principalmente le tipologie di dati e di informazioni oggetto dell'accesso e delimita le finalità (solo la prevenzione e repressione dei reati connessi all'utilizzo di carte di credito o di altri mezzi di pagamento).

I profili di sicurezza sono disciplinati in termini simili a quelli del precedente parere. In particolare il Ced deve impartire al personale abilitato direttive sulle responsabilità connesse all'accesso improprio alla banca dati ed all'uso illegittimo delle informazioni, non può duplicare le informazioni acquisite, né utilizzare dispositivi automatici per la consultazione dei dati in forma massiva; per quanto concerne la sicurezza, è previsto, tra l'altro, l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia nel flusso dei dati.

Il Garante ha espresso parere favorevole sulla Convenzione valutando il suo contenuto conforme alla disciplina in materia di protezione di dati.

Accertamenti di un commissariato sulla situazione debitoria di un cittadino

Di carattere individuale, invece, la decisione relativa alla segnalazione di un cittadino, debitore delle spese di giudizio per un contenzioso civile con una pubblica amministrazione, convocato da un commissariato di polizia per fornire notizie sulla sua situazione economica, in vista di un'eventuale procedura esecutiva a suo carico.

Al riguardo, il Garante ha osservato che l'acquisizione di tali notizie non rientra tra i compiti istituzionali della polizia di Stato e quindi viola le norme del Codice, che ammettono il trattamento e la comunicazione di dati da parte di soggetti pubblici sul fondamento di adeguata normativa o, in mancanza, per lo svolgimento delle funzioni istituzionali (artt. 18, comma 2 e 19, comma 2).

Il trattamento è stato pertanto dichiarato illecito con divieto di ogni ulteriore operazione da

parte del commissariato e dell'ente pubblico creditore, salva la valutazione della sussistenza dei presupposti per la contestazione di violazioni amministrative (provv. 4 ottobre 2012).

1.2. ATTIVITÀ FISCALE E TRIBUTARIA

L'Autorità ha altresì adottato alcuni pareri relativi ad atti dell'amministrazione finanziaria volti al contrasto dell'evasione fiscale, caratterizzati da un complesso intreccio tra profili amministrativi e tecnici.

Agenzia delle entrate - Anagrafe tributaria

In particolare il Garante si è espresso sullo schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità con le quali le banche dovranno comunicare all'Agenzia le informazioni relative ai conti correnti bancari (saldo iniziale e finale, importi totali degli accrediti e degli addebiti delle numerose tipologie di operazioni effettuate) (parere 17 aprile 2012 [doc. web n. 1886775]).

Tali dati dovranno poi essere ordinati su scala nazionale, a mezzo di procedure centralizzate, per la formazione di specifiche liste dei contribuenti a maggior rischio di evasione, secondo i criteri successivamente individuati dall'Agenzia.

Il Garante ha anzitutto evidenziato che la normativa pone rilevanti problemi, sia con riferimento all'eccezionale concentrazione presso l'Anagrafe tributaria di un'enorme quantità di informazioni personali, sia in relazione alle finalità di classificazione degli interessati, cui la raccolta di tali informazioni risulta preordinata. Ha al riguardo ribadito quanto rappresentato in sede di audizione presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria, sottolineando che non è in discussione l'esigenza di disporre delle informazioni necessarie per contrastare l'evasione fiscale, bensì l'integrale duplicazione presso l'Anagrafe stessa di una moltitudine di dati, che genera un incremento esponenziale dei rischi. Ha pertanto prescritto, per la trasmissione e la conservazione dei dati, misure di sicurezza di natura organizzativa e tecnica particolarmente rigorose.

Partecipazione dei comuni alla lotta all'evasione

In pari data l'Autorità ha dato parere favorevole ad un schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità di partecipazione all'accertamento fiscale e contributivo da parte dei comuni, in attuazione della normativa di settore (v. da ultimo art. 18 del d.l. n. 78 del 31 maggio 2010, convertito dalla l. 30 luglio 2010, n. 122).

Il Garante ha espresso parere favorevole a condizione che -per tutti i soggetti coinvolti nel trattamento- siano garantiti *standard* di sicurezza minimi non inferiori a quelli già garantiti dall'Agenzia delle entrate in conformità al provvedimento del 18 settembre 2008 [doc. web n. 1549548].

In particolare ha stabilito che i comuni devono designare responsabili del trattamento i soggetti esterni dei quali decidano di avvalersi, fornendo loro adeguate istruzioni e vigilando sul trattamento tramite verifiche periodiche, anche a campione. Qualora tali soggetti siano designati responsabili da più comuni, non deve essere consentita la correlazione tra informazioni di competenza di comuni diversi (provv. 17 aprile 2012 [doc. web n. 1886825]).

Anagrafe tributaria - trasmissione e conservazione dei dati da parte di banche e operatori finanziari

Nell'ottobre 2012, l'Agenzia delle entrate ha trasmesso un nuovo schema di provvedimento, volto a regolare le modalità della comunicazione integrativa annuale all'archivio dei rapporti finanziari, sulla base delle osservazioni formulate dall'Autorità nel menzionato parere del 17 aprile 2012 [doc. web n. 1886775].

In particolare lo schema disciplina una nuova infrastruttura per la trasmissione dei dati, il "sistema di interscambio" che consente di automatizzare la raccolta dei dati presso gli operatori finanziari, riducendo i passaggi manuali che aumentano, di per sé, le possibilità di accessi non autorizzati.

Tuttavia, poiché l'architettura del sistema non è in grado di escludere interventi umani e prevede la possibilità di passaggi intermedi il Garante, nell'esprimere parere favorevole, ha in particolare chiesto all'Agenzia di adottare alcune misure di sicurezza, prevedendo anzitutto che il protocollo utilizzato per l'intercambio dei dati sia cifrato. L'Autorità ha inoltre individuato le misure da adottare per minimizzare i rischi di accessi abusivi e trattamenti non consentiti, tenendo conto delle esigenze dei piccoli operatori. Trascorso il termine previsto per la loro conservazione, i dati verranno automaticamente cancellati.

Il Garante ha in ogni caso previsto la procedura di verifica preliminare per ogni ulteriore utilizzo dei dati per altre finalità (ad es., controlli Isee) (parere 15 novembre 2012 [doc. web n. 2099774]).

1.3. GIORNALISMO

Il bilanciamento tra la libertà di espressione e le esigenze di protezione dei dati personali ha caratterizzato le deliberazioni in materia di attività giornalistica ed informazione *online.*

Immagini relative all'arresto di persone indagate

Con riferimento ad una trasmissione televisiva che dava conto di indagini coordinate da una Direzione antimafia, il Garante ha vietato l'ulteriore diffusione delle immagini delle persone indagate ritratte all'interno delle proprie abitazioni private -anche attraverso l'utilizzo di cd. "primi piani"- nel momento delicatissimo dell'arresto, ritenendo travalicati i limiti posti dall'ordinamento all'esercizio del diritto di cronaca, in particolare il principio di tutela della dignità della persona e il principio di essenzialità dell'informazione rispetto a fatti di interesse pubblico (provv. 18 maggio 2012 [doc. web n. 1900914]).

Trattamento eccedente dell'immagine di dipendenti pubblici

Due provvedimenti, adottati su reclamo degli interessati, hanno riguardato casi in cui le immagini riconoscibili di dipendenti pubblici (non inquadrabili nella categoria delle cd. "persone note"), che svolgevano i propri compiti in un'aula parlamentare, erano state pubblicate, rispettivamente, su un quotidiano nazionale e diffuse da un servizio televisivo.

Nel primo caso l'Autorità ha ritenuto legittima la pubblicazione delle immagini, lecitamente raccolte, finalizzata alla individuazione visiva degli appartenenti a categorie professionali il cui trattamento giuridico ed economico è oggetto di un dibattito pubblico (provv. 15 novembre 2012 [doc. web n. 2247923]).

Nel secondo, è stata invece ritenuta illegittima la pubblicazione -anche in ragione delle tecniche di ripresa utilizzate- di immagini individualizzate del reclamante, presentato quasi come "emblema" di un'intera categoria. Non è stato tuttavia adottato alcun provvedimento inibitorio, considerata la spontanea decisione del titolare del trattamento di rimuovere dal sito e dai propri archivi le predette immagini (provv. 15 novembre 2012 [doc. web n. 2185342]).

Correttezza del trattamento e aggiornamento di notizie

Anche a seguito della sentenza della Corte di Cassazione n. 5525/2012 sul cd. "diritto all'oblio", la quale ha evidenziato l'esigenza di dar conto dei successivi sviluppi di una vicenda oggetto di informazione poiché "*altrimenti la notizia, originariamente completa e vera, diviene non aggiornata risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera*", il Garante ha accolto due ricorsi che richiedevano di aggiornare, sulla base di sviluppi avvenuti *medio tempore*, articoli (già deindicizzati) presenti sul sito di un'importante testata

giornalistica. In particolare è stato prescritto all'editore di segnalare -ad es. con un'annotazione a margine dei singoli articoli- l'esistenza dello "sviluppo" della notizia, in modo da assicurare da un lato, all'interessato, il rispetto della propria attuale identità personale, e dall'altro, ad ogni lettore, un'informazione attendibile e completa (provv.ti 20 dicembre 2012 [doc. web n. 2286432] e 24 gennaio 2013 [doc. web n. 2286820]).

Procedimento di ricorso e organi costituzionali

Per alcuni profili connessa alla precedente è la problematica relativa alla disponibilità in rete della documentazione dell'attività svolta dalle Camere nelle legislature repubblicane comprendente una massa di dati personali spesso delicati, anche quando non sensibili. Al riguardo, in più occasioni, persone citate in atti parlamentari hanno chiesto di sottrarre i dati in parola all'azione dei motori di ricerca, ovvero di integrare notizie inesatte o incomplete. Gli organi parlamentari, pur richiamando la piena autonomia e insindacabilità nell'esercizio delle funzioni e delle prerogative parlamentari, nel 2012 hanno in particolare invocato il disposto dell'art. 8, comma 2, lettera *c)*, del Codice, che preclude l'utilizzo dello strumento del ricorso nei confronti dei trattamenti svolti da Commissioni parlamentari d'inchiesta.

Il Garante, nel condividere tale impostazione, e ritenendo pertanto inammissibile un ricorso in materia (provv. 19 luglio 2012 [doc. web n. 2065905]), non ha però cessato di ricercare un equilibrio più avanzato, anche alla luce della pur limitata giurisprudenza di merito (v. Trib. Civ. di Roma, 1ª sez., sentenza 19 gennaio 2012). Da qui uno scambio di note fra il Presidente della Camera dei deputati e il Presidente dell'Autorità allo scopo di promuovere ulteriori approfondimenti, volti ad individuare misure (quali la deindicizzazione dei testi) idonee ad evitare che, attraverso la pubblicazione *online* di atti parlamentari, si possano ledere diritti e libertà fondamentali.

1.4. SANITÀ

In questa materia si segnalano due deliberazioni di carattere generale, riguardanti principalmente la "gestione" dei dati da parte delle amministrazioni competenti.

Regolamento sul trattamento di dati sensibili da parte delle regioni

Più in dettaglio, il Garante ha espresso parere favorevole sullo schema tipo di regolamento per il trattamento di dati sensibili e giudiziari da parte di regioni, province autonome ed aziende sanitarie, volto a garantire un più ampio quadro di tutele rispetto ai flussi crescenti di

dati scambiati tra le pubbliche amministrazioni, anche per monitorare il buon andamento dell'attività amministrativa.

Nell'esprimere il parere, l'Autorità ha chiesto che lo schema venga integrato con specifiche garanzie, in particolare prevedendo la codificazione dei dati acquisiti dalle regioni ai fini di monitoraggio e valutazione dei trattamenti sanitari erogati, per evitare l'identificazione diretta del soggetto interessato. Le regioni e le province autonome che intendono aggiornare, sulla base del nuovo schema tipo, i propri atti regolamentari sono tenute a recepire le indicazioni formulate dal Garante nel parere.

Nello stesso atto l'Autorità ha espresso le sue valutazioni sul decreto del Ministero della salute concernente il sistema di sorveglianza delle nuove diagnosi di infezioni da HIV, richiamato dallo schema tipo e viziato per violazione di legge, in quanto emanato senza il previsto parere del Garante (v. art. 154, comma 4, del Codice).

Al riguardo, l'Autorità ha precisato che i trattamenti di dati sensibili possono essere effettuati nell'ambito delle attività amministrative correlate alla sorveglianza epidemiologica dei casi di infezione da HIV, nel rispetto delle specifiche cautele che saranno individuate dal Ministero, in collaborazione con l'Autorità, nel quadro di un percorso collaborativo che il Ministero intende avviare ai fini della revisione del decreto e dell'acquisizione del previsto parere.

Per quanto riguarda i nuovi flussi di dati tra i medici prescrittori e il Ministero dell'economia e delle finanze (Mef), per il monitoraggio della spesa sanitaria, è stata infine rilevata l'esigenza di modificare il protocollo, adottato previo parere dell'Autorità, con cui sono individuati sia i dati in possesso del Mef che possono essere trasmessi al Ministero della salute e alle regioni, sia le modalità di tale trasmissione (comma 10, dell'art. 50 del d.l. 20 settembre 2003, n. 269 (convertito dalla l. 24 novembre 2003, n. 326). Ciò, al fine di estendere le cautele previste dal protocollo per i flussi di dati relativi alle prescrizioni di farmaci e alle prestazioni specialistiche ai nuovi flussi originati dai medici prescrittori (provv. 26 luglio 2012 [doc. web n. 1915390]).

Registro dei tumori del Veneto

Di ambito più circoscritto, ma su materia che presenta profili di estrema delicatezza, il parere rilasciato alla Regione Veneto sullo schema di regolamento recante norme per il

funzionamento del Registro dei tumori (provv. 13 settembre 2012 [doc. web n. 1927415]) in attuazione della l.r. 16 febbraio 2010 n. 11, che prevede l'istituzione di diversi registri di interesse sanitario.

Il regolamento individua il titolare del trattamento dei dati contenuti nel Registro, gli scopi perseguiti nell'ambito della più ampia finalità di ricerca scientifica, i tipi di dati sensibili trattati, i soggetti tenuti ad alimentare il Registro, nonché l'ambito di comunicazione e di diffusione dei dati ivi contenuti (v. art. 18, comma 2, della l.r. n. 11/2010 cit. e artt. 20 e 98 del Codice).

Le osservazioni dell'Ufficio hanno riguardato, in particolare, il rispetto del principio di indispensabilità nel trattamento dei dati, anche con riferimento alla loro conservazione; l'esigenza di utilizzare codici identificativi per tutelare l'identità e la riservatezza dei malati; le cautele per comunicare i dati ai registri tumori di altre regioni, le modalità per dare l'informativa agli interessati, la specificazione di misure organizzative e di accorgimenti tecnici idonei a garantire un adeguato livello di sicurezza dei dati, tra le quali l'obbligo, per il personale incaricato di trattarli, di rispettare regole di condotta analoghe al segreto professionale, anche quando non sia a ciò tenuto per legge.

1.5. COMUNICAZIONI E RETI TELEMATICHE

Di diretta derivazione comunitaria, l'attività in questo settore si caratterizza per atti di rilievo generale.

Schema di d.lgs. di attuazione della Direttiva n. 2009/136/CE

In primo luogo si menziona il parere espresso su richiesta del Ministro dello sviluppo economico e delle infrastrutture e trasporti, sullo schema di d.lgs. n. 69/2012, recante, tra l'altro, modifiche al Codice, in attuazione della Direttiva n. 2009/136/CE, in materia di reti e di servizi di comunicazione elettronica (provv. 29 marzo 2012 [doc. web n. 1893400]).

In estrema sintesi, tra le più rilevanti innovazioni si segnala la disciplina del *data breach*, o violazione di dati personali, che comporta anche accidentalmente la perdita, la modifica o la rivelazione non autorizzata di dati trattati nella fornitura di un servizio di comunicazione elettronica.

In relazione ai *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente), il

testo prevede modalità semplificate per l'espressione del consenso dell'interessato, sulla base di un'informativa a sua volta semplificata.

Nell'esprimere parere favorevole, il Garante ha tra l'altro rilevato, in forma di osservazione (poi recepita nel testo definitivo), l'esigenza di garantire -in merito alla nuova disciplina della raccolta di informazioni nei riguardi dell'abbonato e dell'utente *ex* art. 122 del Codice- l'effettività del diritto dell'interessato ad essere informato in ordine agli scopi del trattamento, se del caso con modalità opportunamente semplificate. Inoltre, è stato suggerito di chiarire che il d.l. n. 201/2011 convertito, con modificazioni, dalla l. n. 214 del 2011 (cd. "salva Italia"), nell'escludere persone giuridiche, enti o associazioni dall'ambito di applicazione del Codice, non ha modificato la definizione di "abbonato" contenuta nel Codice, che risulterebbe perciò -ad avviso del Garante- tuttora applicabile tanto alle persone fisiche quanto a quelle giuridiche.

Non essendo stato accolto tale suggerimento il Garante, con provvedimento di natura interpretativa, ha chiarito che i predetti soggetti continuano a non poter essere contattati se iscritti nel Registro delle opposizioni, né possono ricevere, senza consenso specifico per la finalità promozionale, telefonate automatizzate con messaggi preregistrati, e-mail, fax, sms, mms (provv. 20 settembre 2012 [doc. web n. 2094932]).

Linee-guida sulla comunicazione delle violazioni di dati personali

Gli adempimenti da effettuarsi in occasione di un *data breach* sono poi stati disciplinati in dettaglio nelle linee-guida recanti prescrizioni nei confronti dei fornitori, con particolare riguardo: all'individuazione dei soggetti obbligati a effettuare la comunicazione della violazione; alle circostanze in cui sussiste tale obbligo; all'avviso da dare agli utenti; alle misure di sicurezza tecniche e organizzative da adottare. In particolare, è stato chiarito che sono tenuti a comunicare i *data breach* esclusivamente i fornitori di servizi telefonici e di accesso a internet, e non le reti aziendali, gli internet *point*, i motori di ricerca, i siti internet che diffondono contenuti (provv. 26 luglio 2012, in G.U. 7 agosto 2012, n. 183 [doc. web n. 1915485]).

Informativa relativa ai *cookie* - consultazione pubblica

Come accennato, la disciplina relativa all'uso dei cd. "*cookie*" e degli altri strumenti analoghi (quali *web beacon/web bug, clear* GIF), è stata modificata, a seguito dell'attuazione della Direttiva n. 2009/136/CE ad opera del d.lgs. 28 maggio 2012, n. 69.

In particolare, l'archiviazione delle informazioni nell'apparecchio terminale di un utente o l'accesso a informazioni già archiviate, è consentito se l'interessato ha espresso il suo consenso sulla base di un'informativa semplificata, anche tramite specifiche configurazioni di programmi informatici o di dispositivi di facile e chiara utilizzabilità (v. nuovo testo art. 122 Codice).

Per individuare le modalità semplificate con cui rendere l'informativa *online* sull'utilizzo dei suindicati dispositivi, il Garante ha avviato una consultazione pubblica (provv. 22 novembre 2012, in G.U. 19 dicembre 2012, n. 295 [doc. web n. 2139697]).

1.6. LAVORO

In materia di lavoro la casistica è principalmente relativa a singoli trattamenti, spesso in relazione a segnalazioni degli interessati.

Protocollo informatico

In particolare, in un caso l'Autorità ha chiarito che le informazioni relative ai dipendenti acquisite nel protocollo informatico devono essere accessibili al solo personale specificamente incaricato di tali trattamenti e non alla generalità indifferenziata degli utenti dei servizi di protocollo. Nella vicenda oggetto di accertamenti un ampio numero di dipendenti poteva venire a conoscenza di dati personali di colleghi (quali permessi accordati in base alla l. n. 104/1992, permessi studio, ovvero contestazioni disciplinari), indipendentemente dalle mansioni svolte.

È stato pertanto prescritto, in particolare, di limitare la visibilità degli atti relativi al personale ai soli dipendenti incaricati del loro trattamento (provv. 11 ottobre 2012 [doc. web n. 2097560]).

Impiego di sistemi di videosorveglianza

In un altro caso, a seguito degli accertamenti effettuati presso un *call center*, il Garante ha vietato il trattamento dei dati rilevati mediante un sistema di videosorveglianza in grado di captare anche le conversazioni dei dipendenti (provv. 4 ottobre 2012 [doc. web n. 2066968]), effettuato peraltro in violazione dell'art. 4, l. n. 300/1970. Provvedimenti di analogo contenuto sono stati adottati in presenza di trattamenti effettuati mediante sistemi di videosorveglianza presso un hotel (provv. 25 ottobre 2012 [doc. web n. 2212826]) e un esercizio commerciale (provv. 25 ottobre 2012 [doc. web n. 2212623]), in assenza delle garanzie dettate dall'art. 4, l. n. 300/1970.

In altra fattispecie il Garante ha dichiarato l'illiceità e disposto il blocco del trattamento effettuato dal sistema di videosorveglianza, installato per finalità antitaccheggio presso un esercizio commerciale, mediante una telecamera che riprendeva anche l'area nella quale è posta l'apparecchiatura per la rilevazione delle presenze dei lavoratori (provv. 17 gennaio 2013 [doc. web n. 2291893]).

È stata anche ritenuta inidonea l'informativa fornita agli interessati (pur nelle forme semplificate indicate dall'Autorità nel provvedimento generale dell'8 aprile 2010 [doc. web n. 1712680]) ed è stata altresì riscontrata la possibilità di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali (in violazione dei princìpi di liceità e correttezza nel trattamento).

Un ulteriore profilo di illiceità del trattamento è stato rilevato nella circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa dal titolare del trattamento, è risultato privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773 (Tulps)), come confermato peraltro dal consolidato indirizzo interpretativo della giurisprudenza di legittimità secondo cui "*ogni forma di attività imprenditoriale di vigilanza e custodia di beni per conto terzi esige la licenza del prefetto, indipendentemente dalle modalità operative con le quali viene espletata*" (cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821, con ulteriori richiami).

Installazione di un sistema di registrazione di immagini su veicolo di trasporto locale

Nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha invece ritenuto lecita, da parte di una concessionaria del servizio di trasporto pubblico locale, l'installazione di un dispositivo sul parabrezza delle vetture, che consente di registrare e -al verificarsi di predeterminate "anomalie"- conservare, immagini relative sia all'interno che all'esterno del veicolo. Le finalità perseguite dalla società (salvaguardia del patrimonio aziendale nonché ricostruzione della dinamica di eventuali sinistri in vista della tutela dei diritti in giudizio) e le concrete modalità di trattamento dei dati (esclusione dell'immagine del conducente dall'angolo di ripresa, offuscamento dei volti di soggetti terzi non coinvolti negli eventi) sono state infatti ritenute conformi ai princìpi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *d)*, del Codice). Sono state invece ritenute eccedenti, rispetto alle finalità rappresentate, la raccolta e conservazione -pure prospettata dalla società- di registrazioni della

voce delle persone a bordo del veicolo, anche alla luce della sua possibile rilevanza penale (cfr. artt. 617, 617-*bis* e 623-*bis* c.p.) (provv. 29 novembre 2012 [doc. web n. 2257616]).

Operatori di un *call center* e controlli di qualità

L'Autorità ha altresì effettuato accertamenti in relazione sia alla registrazione e al riascolto delle telefonate degli operatori di un *call center* gestito da una cooperativa, sia al monitoraggio della condotta tenuta dagli stessi operatori mediante l'analisi del numero e della durata delle conversazioni.

Al riguardo, poiché la registrazione ed il riascolto delle comunicazioni consentono il controllo a distanza dell'attività dei lavoratori, il Garante ha rilevato che il mancato assolvimento degli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 (fatto salvo dall'art. 114 del Codice) riverbera i propri effetti anche sulle operazioni di trattamento, le quali risultavano perciò in violazione dell'art. 11, comma 1, lett. *a)*, del Codice. Analoga la valutazione sul monitoraggio delle conversazioni di ciascun operatore telefonico in base al loro numero o durata, non essendo stati posti in essere gli adempimenti previsti dal cit. art. 4 (provv. 1° agosto 2012 [doc. web n. 1923325]; in materia provv. 9 febbraio 2011 [doc. web n. 1797032]).

Rilevazione dati biometrici per controllo delle presenze dei dipendenti

Sempre in sede di verifica preliminare è stata esaminata l'istanza di un comune, per l'installazione di un sistema di rilevazione biometrica delle presenze dei dipendenti, basato sulla lettura delle impronte digitali, volta ad impedire usi impropri del *badge*. Il Garante ha ritenuto non conforme ai princìpi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3, 11, comma 1, lett. *d*), del Codice) il trattamento, poiché l'ente locale non aveva comprovato l'insufficienza delle ordinarie modalità di controllo, in alternativa ai più invasivi sistemi biometrici (provv. 31 gennaio 2013 [doc. web n. 2304669].

Trattamento di dati sensibili riferiti ai partecipanti ad una manifestazione sindacale

È stato altresì ritenuto illecito il trattamento, da parte di una casa circondariale, dei nominativi del personale di polizia penitenziaria che aveva preso parte ad una manifestazione sindacale (provv. 29 novembre 2012 [doc. web n. 2192643]).

Il trattamento, pur se (in astratto) consentito ai fini di un eventuale procedimento disciplinare, non risultava in concreto lecito, poiché la mera indizione e partecipazione ad una manifestazione sindacale non configura alcun illecito, alla luce della fondamentale libertà di riunione riconosciuta dall'art. 17 della Costituzione nonché dalla normativa di settore (v. art. 19, l. n. 395/1990 recante l'ordinamento del Corpo di polizia penitenziaria).

È stato pertanto prescritto alla casa circondariale -che si è tempestivamente conformata- il divieto di trattare ulteriormente i nominativi dei partecipanti alla manifestazione, nonché di portare a conoscenza dei soggetti, cui eventualmente i dati fossero stati comunicati, in particolare, l'inutilizzabilità dei dati stessi (provv. 29 novembre 2012 [doc. web n. 2192643]).

Consegna di comunicazioni ai lavoratori

In più di una circostanza, l'Autorità è stata chiamata a pronunciarsi in relazione alla notifica a mano di comunicazioni contenenti dati personali del lavoratore: tali sono stati considerati dal Garante anche i dati quantitativi e qualitativi riferiti allo svolgimento delle attività professionali che, nella fattispecie considerata, pur facendo complessivamente capo ad un'unità organizzativa, rientravano comunque nelle attribuzioni della reclamante (che ne era responsabile) (provv. 18 ottobre 2012 [doc. web n. 2174351]). Tale valutazione in merito alla nozione di dato personale è peraltro conforme a quella del Gruppo Art. 29 (Parere n. 4/2007, adottato il 20 giugno 2007 - WP 136, p. 6 e ss. [doc. web. n. 1607426]).

Da un altro caso è emerso con chiarezza che l'interesse del titolare del trattamento -specie riguardo ad atti dalla cui ricezione decorrono particolari effetti- a formare la prova dell'avvenuta ricezione mediante sottoscrizione del destinatario su copia degli atti, richiede l'adozione di adeguate cautele, tra le quali l'individuazione dell'incaricato in una persona già a conoscenza del contenuto per ragioni di ufficio. Si trattava della notifica di determinazioni aventi ad oggetto l'irrogazione di sanzioni disciplinari ad un lavoratore da parte del proprio superiore gerarchico (provv. 18 ottobre 2012 [doc. web n. 2174582]).

Accordo tra la Repubblica italiana e lo Stato di Israele sulla previdenza sociale

Connesso con la materia del lavoro è il parere espresso, su richiesta del Ministero degli affari esteri, su uno schema di d.d.l. recante la ratifica ed esecuzione di un accordo con lo Stato di Israele che, per garantire ai cittadini italiani ivi trasferitisi una pensione in linea con i contributi versati in Italia, prevede una comunicazione di dati da parte del Ministero del lavoro e delle politiche sociali ad altro soggetto straniero (e viceversa).

In proposito occorre tenere presente che il trasferimento di dati personali verso Paesi terzi può avvenire, tra l'altro, in base alle decisioni con le quali la Commissione europea constata che il Paese terzo garantisce un adeguato livello di protezione dei dati personali (art. 44, comma 1, lett. *b)*, del Codice).

Al riguardo, la decisione della Commissione europea del 31 gennaio 2011 n. 2011/61/UE ha ritenuto adeguato il livello di protezione assicurato nello Stato d'Israele -come definito ai sensi del diritto internazionale- ai trattamenti automatizzati, ai quali soli si applica la legge israeliana sulla protezione della vita privata (considerando n. 9 della citata Decisione). Il Garante aveva quindi autorizzato i trasferimenti di dati verso lo Stato d'Israele, in conformità alla suddetta Decisione (provv. 20 gennaio 2012 [doc. web n. 1868817]) ed ha conseguentemente espresso parere favorevole sul testo del d.d.l. (provv. 25 ottobre 2012 [doc. web n. 2185056]).

1.7. DIRITTI DELL'INTERESSATO E CORRETTEZZA DEL TRATTAMENTO

Si segnalano, ancora, tre casi che evidenziano profili di protezione di situazioni giuridiche soggettive in relazione a trattamenti posti in essere da soggetti pubblici.

Adozione ed attestazioni di stato civile

Attiene ad un delicatissimo ambito della sfera familiare il caso di una persona che contestava ad un comune di aver rilasciato a un avvocato, che agiva privo di delega per conto di alcuni parenti dell'interessato, la copia integrale del suo atto di nascita recante le informazioni sul provvedimento giudiziario riguardante la sua adozione.

L'Autorità ha al riguardo evidenziato che qualunque attestazione di stato civile riferita all'adottato può essere rilasciata solo con l'indicazione del nuovo cognome e con l'esclusione di qualsiasi riferimento alla paternità e alla maternità del minore, poiché indicazioni sul rapporto di adozione possono essere fornite solo su espressa autorizzazione dell'autorità giudiziaria (artt. 26, comma 4, e 28, comma 2, l. 4 maggio 1983, n. 184; artt. 106 e 107, commi 1 e 2, lett. *b*), d.P.R. 3 novembre 2000, n. 396; art. 177, comma 3, del Codice).

È stato quindi vietato ai parenti dell'interessato l'ulteriore utilizzo delle predette informazioni sull'adozione e prescritto al comune di fornire al personale di stato civile adeguate istruzioni per evitare ulteriori violazioni in materia (provv. 8 novembre 2012 [doc. web n. 2187244]).

Rettificazione di sesso su certificazioni di laurea

Riguarda la protezione della sfera personalissima il caso nel quale uno studente laureato ha chiesto chiarimenti sulla possibilità di ottenere, a seguito dell'avvenuta rettificazione di attribuzione di sesso, un nuovo diploma di laurea, indicante solo i nuovi dati anagrafici. Contestualmente, l'università ha rappresentato al Garante la propria intenzione di rilasciare tale secondo diploma, senza dar conto delle ragioni della ristampa. Questa soluzione è

apparsa all'Autorità idonea a tutelare la dignità degli interessati e il loro diritto a vedere correttamente rappresentata la loro attuale identità sessuale. Il Garante ha pertanto prescritto a tutte le università, nell'ambito della loro autonomia -fermi restando gli obblighi di conservazione dell'atto originario- l'adozione di idonei accorgimenti, affinché non siano riportate nella relativa documentazione elementi idonei a rivelare l'avvenuta rettificazione di attribuzione di sesso (provv. 15 novembre 2012 [doc. web n. 2121695]).

Punti patente

Si segnala ancora l'istanza di un cittadino, che lamentava la mancata registrazione, presso l'Anagrafe nazionale degli abilitati alla guida, della totalità delle annotazioni, comportanti variazione del punteggio della patente (decurtazioni e attribuzioni di punti).

Dalla documentazione prodotta è emerso che la comunicazione effettuata dal Ministero delle infrastrutture e dei trasporti non conteneva talune variazioni di punteggio, che non erano annotate neppure nell'estratto conto dei punti, consultabile nel portale di servizi di *e-government* del Dipartimento trasporti del Ministero, in contrasto con la disciplina di settore e con la regola secondo la quale le informazioni personali -anche quelle contenute in banche dati pubbliche- devono essere trattate secondo correttezza, esatte e, se necessario, aggiornate (art. 11, comma 1, lett. *a)*, *c)*, *d),* del Codice).

Il Garante ha pertanto prescritto al Ministero che le comunicazioni agli interessati (anche nel caso di consultazione diretta del cd. "portale dell'automobilista") contengano i dati relativi alla totalità delle variazioni, comprese quelle effettuate in modo automatizzato, di attribuzione di punti (*bonus*) e successiva decurtazione per illegittima attribuzione e, anche per quanto riguarda gli eventi passati, che, qualora l'interessato ne faccia specifica richiesta, sia assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazioni (provv. 24 gennaio 2013 [doc. web n. 2256617]).

1.8. PROGRAMMA STATISTICO NAZIONALE 2011-2013

Nel 2012 su richiesta dell'Istat, l'Autorità si è espressa in relazione al trattamento di dati personali inseriti per la prima volta nel Programma statistico nazionale (Psn) 2011-2013, Aggiornamento 2013, e alle modifiche apportate ai prospetti identificativi di lavori statistici, già inclusi nel precedente Programma 2011-2013 e nel relativo Aggiornamento 2012-2013 (parere 9 febbraio 2012 [doc. web n. 1876517]).

In primo luogo, il Garante ha preso atto del mancato adeguamento alle modifiche normative che hanno sottratto all'ambito di applicazione della disciplina in materia di protezione dati le informazioni relative a persone giuridiche, enti e associazioni. Sul punto l'Autorità ha raccomandato, in vista della redazione del Psn 2014-2016, di prestare particolare attenzione ai lavori statistici che, pur concernendo prevalentemente persone giuridiche, possono comportare il trattamento di dati personali riferiti a persone fisiche (quali le attività professionali svolte in forma individuale).

Inoltre sono state evidenziate specifiche criticità con riferimento agli studi progettuali del Ministero del lavoro e delle politiche sociali che prevedono, in particolare, la trasmissione al sistema informativo dell'Inps di informazioni trattate a fini amministrativi dai comuni, corredate di dati identificativi diretti e di informazioni molto delicate, relative anche allo stato di salute e alla vita sessuale dei minori.

Al riguardo, l'Autorità ha, tra l'altro, evidenziato che i dati personali trattati a fini statistici non possono essere utilizzati per scopi di altra natura e che il trattamento dei dati sensibili e giudiziari in parola non è previsto allo stato da alcuna norma di legge che individui i tipi di dati e le operazioni eseguibili, condizionando pertanto il parere favorevole sul Psn 2011-2013, Aggiornamento 2013, all'eliminazione dallo stesso dei predetti studi progettuali (parere 20 settembre 2012 [doc. web n. 2069239]).

1.9. PROPAGANDA ELETTORALE

In prossimità delle elezioni amministrative del 2012 e delle politiche del 2013 con due provvedimenti sono stati previsti speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati, individuando le corrette modalità in base alle quali tali soggetti possono utilizzare a fini di propaganda elettorale i dati dei cittadini (provv.ti 5 aprile 2012 [doc. web n. 1885765] e 10 gennaio 2013 [doc. web n. 2181429]).

È stato così ricordato, in particolare, che possono essere usati senza il consenso dei cittadini i dati contenuti nelle liste elettorali detenute dai comuni, nell'elenco degli elettori residenti all'estero, o in altre fonti documentali detenute da soggetti pubblici accessibili a

chiunque, nonché i dati di iscritti ed aderenti e quelli raccolti nel quadro di relazioni interpersonali con cittadini ed elettori.

Il consenso è necessario segnatamente per utilizzare i dati raccolti su internet, per contattare gli abbonati presenti negli elenchi telefonici e per l'utilizzo di particolari modalità di comunicazione elettronica (quali sms, e-mail, telefonate preregistrate). È altresì necessario per l'uso dei dati di simpatizzanti o persone già contattate per singole iniziative politiche (ad es., *referendum*, proposte di legge, raccolte di firme).

Non sono invece utilizzabili, tra gli altri, gli archivi dello stato civile, l'Anagrafe dei residenti, indirizzi raccolti dai soggetti pubblici per svolgere attività e compiti istituzionali. Non possono essere usate neppure le liste elettorali di sezione già utilizzate nei seggi, recanti l'indicazione dei non votanti.

Trascorse le date indicate nei suddetti provvedimenti i soggetti che utilizzano i dati per esclusivi fini di selezione di candidati alle elezioni, di propaganda elettorale e di comunicazione politica possono continuare a trattare i dati personali solo informando gli interessati entro i termini indicati nei provvedimenti stessi.

Si segnala, infine che, nell'ambito delle consultazioni tenutesi nel 2012 per l'individuazione del candidato della coalizione di centro-sinistra alla Presidenza del Consiglio dei ministri (cd. "primarie"), l'Autorità ha esaminato alcuni profili problematici sollevati da un comitato e da alcuni privati cittadini in merito ad alcune disposizioni del relativo regolamento, che richiedeva la sottoscrizione di un "pubblico appello" e l'iscrizione in un apposito "albo", con connessa possibile diffusione di dati sensibili dei partecipanti alle citate consultazioni (provv. 31 ottobre 2012 [doc. web n. 2079275]).

Il Garante, richiamata la natura sensibile dei dati, ha ribadito l'esigenza di attenersi ai princìpi posti dagli artt. 3 e 11 del Codice, invitando altresì il Comitato della coalizione (nella dichiarata veste di titolare del trattamento) ad evitare forme di diffusione dei dati e ad adottare adeguate misure per la sicurezza dei medesimi, ed ha rinviato, per la disciplina dei profili non espressamente considerati, alle disposizioni dell'autorizzazione generale n. 3/2011, sul trattamento dei dati sensibili da parte di associazioni e fondazioni (provv. 24 giugno 2011 [doc. web n. 1822585]).

2. Quadro normativo in materia di protezione dei dati personali

2.1. Le garanzie previste nel Codice e alcuni recenti interventi modificativi

L'applicazione -anche in sede giurisdizionale e amministrativa- del Codice ne ha dimostrato l'assoluta rilevanza in chiave di garanzia dei diritti fondamentali della persona rispetto al trattamento di dati che la riguardano.

L'evoluzione del quadro normativo europeo ha imposto, però, l'adeguamento del Codice ai nuovi princìpi introdotti a livello sovranazionale, in particolare nel settore delle comunicazioni elettroniche (Direttiva n. 2009/136/CE).

Ulteriori, circoscritte modifiche sono ascrivibili ad un provvedimento d'urgenza del Governo (d.l. 9 febbraio 2012, n. 5 convertito, con modificazioni, dalla l. 4 aprile 2012, n. 35) emanato per esigenze di "semplificazione" di taluni adempimenti in materia di sicurezza dei dati e di "copertura normativa" al trattamento di dati giudiziari nel settore della prevenzione e del contrasto dei fenomeni di criminalità organizzata.

Di seguito si illustrano brevemente e partitamente le cennate modifiche.

2.1.1. Modifiche in materia di comunicazioni elettroniche

Le più rilevanti innovazioni alla disciplina in materia di protezione dati sono state introdotte, principalmente sotto forma di novella alle disposizioni del Codice, dal d.lgs. 28 maggio 2012, n. 69, adottato in attuazione delle Direttive n. 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e n. 2009/140/CE in materia di reti e servizi di comunicazione elettronica (art. 9, l. 15 dicembre 2011, n. 217 - legge comunitaria 2010).

Alla stesura del decreto è stato chiamato a collaborare, in via informale, il Garante che ha poi espresso, su richiesta del Governo, motivato parere, fornendo indicazioni per assicurare il rispetto del quadro normativo europeo e nazionale in materia di protezione dati (cfr. *infra* par. 3.1.).

Le disposizioni del decreto legislativo, nel dare attuazione al rinnovato quadro europeo (la citata Direttiva n. 2009/136/CE ha modificato la precedente Direttiva n. 2002/58/CE in

materia, cui il Governo aveva dato attuazione proprio con il d.lgs. n. 196/2003, recante il Codice), introducono significative modifiche al Codice, rispetto ai trattamenti effettuati da fornitori di servizi di comunicazioni elettroniche (Titolo X).

Tra le novità più importanti si segnalano l'introduzione della "violazione di dati personali" (*data breach*), intesa come *"violazione degli obblighi di sicurezza del trattamento che comporta, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico"* (art. 4, comma 3, lett. g-*bis*, del Codice), e gli adempimenti del fornitore del servizio di comunicazione elettronica in caso di violazione dati personali (art. 32-*bis* del Codice*)*. Tali adempimenti consistono, essenzialmente, nella comunicazione dell'evento al Garante, al fine di consentirgli l'esercizio dei propri poteri a tutela degli interessati. Inoltre, qualora l'illecito rischi di "*arrecare pregiudizio ai dati personali o alla vita privata di un contraente o di altra persona*", il fornitore è tenuto a fornire idonea comunicazione anche a tali soggetti.

La nuova fattispecie è incentrata sul pregiudizio alla riservatezza dell'interessato, determinatosi -anche accidentalmente- per una "violazione degli obblighi di sicurezza" nell'ambito della fornitura di un servizio di comunicazione elettronica e nel conseguente onere informativo a carico del fornitore verso il Garante e verso i soggetti interessati. Tuttavia, ai descritti adempimenti non è tenuto il fornitore in grado di dimostrare di aver adottato misure di protezione tali da rendere i dati inintelligibili a chi non sia autorizzato ad accedervi, in virtù di una presunzione relativa di inoffensività della violazione in tali ipotesi. L'inadempimento ai suddetti obblighi realizza un illecito amministrativo punito con sanzioni pecuniarie, differenziate nel *quantum* in ragione della rilevanza dell'obbligo inadempiuto (nuovo art. 162-*ter* del Codice).

Gli adempimenti da effettuarsi in occasione del verificarsi di un *data breach* sono stati poi disciplinati nel dettaglio dalle linee-guida del Garante approvate il 26 luglio 2012 e sottoposte a consultazione pubblica [doc. web n. 1915485].

Altre novità di rilievo riguardano alcune definizioni già recate dal Codice (il *nomen* "abbonato" viene sostituito con "contraente"), la disciplina dell'archiviazione delle informazioni nel terminale del contraente, con particolare riferimento ai cd. "*cookie*" (art. 122), le

misure di sicurezza e procedure a cura dei fornitori di servizi di comunicazione elettronica (artt. 32 e 132-*bis*) e, infine, l'adeguamento dell'impianto sanzionatorio, con il nuovo art. 162-*ter* concernente "la violazione di dati personali", già citato.

Particolarmente interessante è la nuova disciplina della archiviazione delle informazioni nell'apparecchio terminale dell'abbonato (ora "contraente") e dell'utente, nonché dell'accesso a informazioni già archiviate (cd. "*cookie*"). Il decreto, nel modificare l'art. 122 del Codice, pur confermando l'importanza di una scelta consapevole degli utenti della rete e quindi di un loro consenso libero e informato al trattamento dei propri dati personali (cd. "*opt-in*"), ha previsto forme semplificate di informativa e modalità "agevolate" di espressione del consenso stesso.

Nell'esprimere parere favorevole, il Garante ha rilevato, tra l'altro, in forma di osservazione (poi recepita nel testo definitivo del decreto), l'esigenza di garantire l'effettività del diritto dell'interessato ad essere informato in ordine agli scopi del trattamento, a tal fine eliminando la clausola limitativa ("in quanto applicabile") nel rinvio all'art. 13 del Codice contenuta nello schema di decreto. Il Garante ha rilevato infatti come il diritto dell'abbonato e dell'utente ad essere informati ai sensi dell'art. 13 deve essere assicurato nella sua pienezza, a prescindere da ogni valutazione di "applicabilità" o di compatibilità. Interpretando tuttavia le esigenze di semplificazione connesse al contesto di riferimento, il Garante ha suggerito di fare riferimento a forme semplificate di informativa, che agevolino l'adempimento di tale obbligo da parte dei fornitori di servizi di comunicazione elettronica.

Il Garante ha, inoltre, sottolineato l'opportunità di delineare con chiarezza il quadro normativo riferibile alla figura dell'abbonato-persona giuridica nel contesto dei trattamenti disciplinati dal Titolo X del Codice (connessi alla fornitura di servizi di comunicazione elettronica). Il d.l. n. 201 del 2011, convertito, con modificazioni, dalla l. n. 214/2011 (cd. "decreto salva Italia"), nell'escludere persone giuridiche, enti o associazioni dalla sfera dei soggetti di diritto ai fini della protezione dati non ha, infatti, modificato le disposizioni del predetto Titolo X del Codice dedicate al trattamento di dati connesso alla fornitura di servizi di comunicazioni elettronica e, in particolare, in ossequio al quadro normativo europeo, non ha modificato l'oggetto della definizione di "abbonato" pure contenuta nel Codice, che risulta perciò tuttora applicabile tanto alle persone fisiche quanto a quelle giuridiche.

Il Garante ha rilevato, comunque, l'opportunità di un chiarimento espresso sulle garanzie ascrivibili agli abbonati-persone giuridiche, suggerendo tra l'altro di novellare le nozioni stesse di "interessato" e di "dato personale", nelle quali far rientrare, limitatamente al trattamento dei dati nel settore delle comunicazioni elettroniche, rispettivamente, le persone giuridiche, gli enti ed associazioni in quanto "abbonati" ad un servizio di comunicazione elettronica, e i dati relativi a tali soggetti.

Tali suggerimenti non sono stati tuttavia recepiti nel testo definitivo del decreto legislativo; ragione per la quale in data 20 settembre 2012 il Garante ha adottato un provvedimento di natura interpretativa in cui ha dichiarato di ritenere applicabile anche a persone giuridiche, enti ed associazioni il Capo 1 del Titolo X del Codice, *rectius* le disposizioni ivi contenute che riguardano i "*contraenti*", a prescindere dal loro essere persone fisiche ovvero giuridiche, enti ed associazioni (cfr. *infra* par. 11.1.).

2.1.2. Misure di sicurezza

2.1.2.1. La soppressione del documento programmatico sulla sicurezza (dps)

Relativamente alla disciplina delle misure di sicurezza, con il d.l. 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla l. 4 aprile 2012, n. 35 (cd. "decreto semplifica Italia") sono stati soppressi l'obbligo di tenuta del dps e, conseguentemente, la facoltà di sostituzione dello stesso con l'autocertificazione (art. 45, comma 1, lett. *c)* e *d)*).

L'abolizione del dps ha fatto venir meno un importante adempimento a carico dei titolari del trattamento dei dati che, seppur perfettibile, rappresentava in ogni caso una "scadenza" molto utile alle imprese e agli enti pubblici (si doveva aggiornare, infatti, con cadenza annuale) per valutare lo "stato dell'arte" degli adempimenti necessari per garantire la protezione e la sicurezza dei dati nei propri sistemi informativi.

Si tenga conto, poi, che la soppressione di tale adempimento non ha fatto venir meno l'obbligo, per i titolari del trattamento, di adottare tutte le altre misure di sicurezza previste dal Codice, sia, cioè, quelle "adeguate" previste dall'art. 31 del Codice, sia, anche, quelle minime indicate nell'Allegato B. al Codice, diverse e ulteriori rispetto al dps.

2.1.2.2. La semplificazione delle misure di sicurezza

Il medesimo d.l. n. 5/2012 ha fatto venir meno, poi, il potere del Garante di individuare con proprio provvedimento modalità semplificate di applicazione delle misure minime di sicurezza per i trattamenti, tra l'altro, effettuati per correnti finalità "amministrativo-contabili", previsto dal comma 1-*bis* dell'art.34 del Codice, che è stato integralmente abrogato (art. 45, comma 1, lettera *c)*).

La novella del 2011 si era limitata a perfezionare la procedura per l'adozione di tale provvedimento da parte del Garante, inserendo opportunamente l'obbligo di sentire, oltre al Ministro per la semplificazione normativa, anche il Ministro per la pubblica amministrazione e l'innovazione. L'attuale soppressione integrale priva, invece, il settore delle attività svolte per correnti finalità amministrativo-contabili e dei connessi trattamenti di dati della possibilità di avvalersi di semplificazioni, peraltro già individuate dal Garante con il provvedimento del 27 novembre 2008 [doc. web n. 1571218].

La soppressione di tale potere di semplificazione induce, a maggior ragione, a ritenere necessario l'adeguamento, rimesso al Ministero della giustizia, delle misure minime di sicurezza in relazione all'evoluzione tecnica e all'esperienza maturata nel settore, secondo la procedura di cui all'art. 36 del Codice.

2.1.3. Trattamento di dati giudiziari

Il citato d.l. 9 febbraio 2012, n. 5, ha inoltre introdotto alcune disposizioni di rilievo in materia di trattamento di dati giudiziari (art. 45, comma 1, lettere *a)* e *b)*).

In particolare, è ora consentito il trattamento di dati giudiziari in attuazione di protocolli di intesa in materia di prevenzione e contrasto della criminalità organizzata, stipulati con il Ministero dell'interno o con i suoi uffici periferici, che specifichino la tipologia dei dati trattati e delle operazioni eseguibili (artt. 21, comma 1-*bis* e 27 del Codice).

In relazione a tali disposizioni, il Garante aveva fornito al Parlamento, durante l'esame in prima lettura del disegno di legge di conversione, talune osservazioni volte al perfezionamento della disciplina in esame.

In primo luogo, il Garante rilevava l'esigenza di indicare in maniera maggiormente precisa le finalità per il perseguimento delle quali si autorizza il trattamento di dati giudiziari, poiché

la nozione di *"prevenzione e (…) contrasto dei fenomeni di criminalità organizzata"* non circoscrive con precisione le finalità al trattamento.

Una più puntuale indicazione delle finalità per le quali il trattamento è autorizzato *ex lege* avrebbe contribuito -ad avviso del Garante- ad evidenziare il nesso che necessariamente deve sussistere tra lo specifico protocollo stipulato, lo scopo cui esso è preordinato e i soggetti, pubblici e privati, legittimati al trattamento, anche al fine di impedire utilizzazioni abusive di dati personali così delicati e perciò meritevoli di una tutela particolare.

In secondo luogo, il Garante manifestava forti perplessità in ordine alla scelta di demandare la definizione della tipologia dei dati trattati e delle operazioni eseguibili ad atti -quali i protocolli d'intesa- che hanno natura convenzionale, non normativa e comunque equiparabili alle fonti legittimate, ai sensi degli artt. 21 e 27 del Codice, a disciplinare tali aspetti (la stessa legge, il provvedimento del Garante o, per il trattamento effettuato da soggetti pubblici, il regolamento).

Sarebbe stato pertanto preferibile demandare la definizione della tipologia dei dati trattati e delle operazioni eseguibili a un atto di natura regolamentare -previa acquisizione del parere del Garante- cui i protocolli d'intesa avrebbero dovuto poi conformarsi.

In ogni caso, al fine di elevare le garanzie del diritto alla protezione dei dati personali, il Garante sottolineava l'opportunità di prevedere il parere conforme del Garante in ordine ai protocolli d'intesa stipulati con il Ministero dell'interno e destinati a disciplinare in concreto le modalità del trattamento dei dati.

Tale ultima osservazione è stata (sia pure in parte) recepita durante l'esame parlamentare. In sede di conversione, infatti, è stato previsto il parere del Garante in ordine ai suddetti protocolli d'intesa.

Allo stato non risulta pervenuta nessuna richiesta di parere sui protocolli.

2.2. NOVITÀ NORMATIVE CON RIFLESSI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

2.2.1. Leggi di particolare interesse

Nel 2012 sono stati approvati alcuni importanti provvedimenti normativi che hanno riguardato anche il trattamento di dati personali in delicati settori nonché l'attività del Garante.

Si ricordano in particolare:

"Fase ascendente" e "discendente" del diritto europeo

1) la l. 24 dicembre 2012, n. 234, reca norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea (in G.U. 4 gennaio 2013, n. 3).

A seguito del Trattato di Lisbona il provvedimento riforma, tra le altre cose, la cd. "fase ascendente" nonché quella "discendente" degli atti europei, sostituendo integralmente la l. 4 febbraio 2005, n. 11. Tra le disposizioni di interesse, il provvedimento prevede che nella preparazione delle proprie riunioni, il Comitato interministeriale per gli affari europei (Ciae) si avvalga del Comitato tecnico di valutazione degli atti dell'UE operante presso il Dipartimento politiche europee della Presidenza del Consiglio dei ministri, che coordina, nel quadro degli indirizzi del Governo, la predisposizione della posizione italiana nella fase ascendente; alle riunioni del Comitato tecnico di valutazione "*possono essere invitati, quando si trattano questioni che rientrano nelle rispettive competenze, rappresentanti delle autorità di regolamentazione o vigilanza*" (art. 19). Tale previsione è di particolare importanza per le autorità indipendenti come il Garante, perché consente alle stesse di partecipare attivamente alla definizione della posizione italiana nella cd. "fase ascendente";

Legge di stabilità 2013

2) la l. 24 dicembre 2012, n. 228 reca disposizioni per la formazione del bilancio annuale e pluriennale dello stato (legge di stabilità 2013) (in G.U. 29 dicembre 2012, n. 302). Oltre a disciplinare il finanziamento dell'Autorità (stanziamento di bilancio del Garante in Tabella C nonché proroga del comma 241 dell'art. 2 della l. 23 dicembre 2009, n. 191, che prevede il finanziamento "incrociato" tra Autorità indipendenti a favore del Garante, anche per gli anni 2013, 2014 e 2015), la legge disciplina alcuni argomenti di interesse. Tra questi rilevano le disposizioni sul processo telematico e i pubblici elenchi (comma 19) e la disciplina dei trapianti di organi (comma 340 ss). In particolare, la legge prevede che il deposito degli atti processuali debba avvenire esclusivamente con modalità telematiche, mentre per quanto concerne i pubblici elenchi, dispone che a far data dal 15 dicembre 2013, ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa e stragiudiziale, si intendono per pubblici elenchi quelli previsti dagli artt. 4 e 16, comma 12, del d.l. 18 ottobre 2012, n. 179, nonché quelli previsti

dall'art. 16 del d.l. 29 novembre 2008, n. 185, e il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia. Inoltre, la medesima disposizione stabilisce che con decreto del Ministro della giustizia dovrà procedersi all'adeguamento delle regole tecniche sancite da un precedente d.m. 21 febbraio 2011, n. 44. Invece, per quanto attiene alla disciplina del trapianto di organi, la legge in esame, modificando la l. 1° aprile 1999, n. 91, stabilisce che il centro nazionale trapianti, ai fini della protezione dei donatori viventi, nonché della qualità e della sicurezza degli organi destinati al trapianto, sia preposto alla tenuta del registro dei donatori viventi, in conformità alle disposizioni del Codice, precisando, altresì, che il diritto alla protezione dei dati debba essere tutelato in tutte le fasi delle attività di donazione e trapianto degli organi, risultando vietato, a tal fine, qualsivoglia accesso non autorizzato a dati o sistemi tramite il quale sia possibile identificare i donatori o i riceventi. Infine, la legge prevede che, con decreto di natura non regolamentare del Ministro della salute, sia disposta l'adozione e l'attuazione di procedure operative volte, tra l'altro, alla verifica dell'identità del donatore e delle informazioni relative al consenso, a fornire garanzie di tracciabilità nel rispetto delle norme del Codice, nonché finalizzate alla segnalazione, all'esame, alla registrazione e alla trasmissione delle informazioni necessarie, sugli eventi e reazioni gravi, e avversi suscettibili di inficiare la qualità e la sicurezza degli organi;

Decreto cd. "Crescita 2"

3) il d.l. 18 ottobre 2012, n.179, recante misure urgenti per la crescita del Paese (decreto cd. "Crescita 2") convertito dalla l. 17 dicembre 2012, n. 221. Molte delle norme introdotte dal decreto-legge hanno un impatto significativo sulla materia della protezione dei dati personali, in quanto comportano la creazione di nuove banche-dati e di ulteriori forme d'interconnessione tra quelle esistenti o autorizzano flussi di dati personali anche di particolare delicatezza quali quelli di carattere sanitario o giudiziario. In conseguenza di ciò, molti dei provvedimenti (regolamenti o decreti aventi natura non regolamentare) cui è demandata la concreta attuazione delle norme primarie prevedono espressamente il parere del Garante o comunque riguardano aspetti di protezione dei dati così da dover essere sottoposti comunque al parere dell'Autorità ai sensi dell'art. 154, comma 4, del Codice.

Si riportano di seguito le disposizioni di maggiore interesse per l'Autorità.

All'interno della sezione "Agenda e identità digitale" -dedicata all'attuazione dell'Agenda Digitale italiana- rilevano disposizioni volte a sviluppare l'identità digitale del cittadino, con riferimento, in particolare, ai seguenti aspetti:

a) (Documento digitale unificato). L'art. 1, comma 2, modificando l'art. 10 del d.l. 13 maggio 2011, n. 70, convertito, con modificazioni, dalla l. 12 luglio 2011, n. 106, prevede che con d.P.C.m., sentita l'Agenzia per l'Italia Digitale, sia disposto, anche progressivamente, l'ampliamento delle possibili utilizzazioni della carta d'identità elettronica anche in relazione all'unificazione con la tessera sanitaria. Le modalità tecniche di produzione, distribuzione e gestione del predetto documento unificato saranno stabilite con apposito decreto del Ministro dell'interno. Al riguardo presso il Ministero dell'interno è stato avviato un tavolo tecnico di lavoro al quale è stato invitato a partecipare in via collaborativa anche il Garante, che sta esaminando le prime bozze di decreti attuativi in vista della formulazione dei pareri di competenza;

b) (Anagrafe nazionale della popolazione residente - Anpr). Mediante sostituzione integrale dell'art. 62 del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - Cad) è istituita l'Anagrafe nazionale della popolazione residente *(*Anpr), quale base di dati di interesse nazionale, destinata a subentrare all'Indice nazionale delle anagrafi (Ina) e all'Anagrafe della popolazione italiana residente all'estero (Aire). La nuova Anagrafe dovrebbe costituire il riferimento informativo per tutte le pubbliche amministrazioni e gli erogatori di pubblici servizi, ai quali assicura l'accesso. A definire tempi e modalità del processo di sostituzione con la nuova Anagrafe nazionale è previsto siano uno o più decreti del Presidente del Consiglio, previo parere del Garante, anche con riferimento "*alle garanzie e alle misure di sicurezza da adottare nel trattamento dei dati personali*", alle modalità e ai tempi di conservazione dei dati e all'accesso agli stessi da parte delle pp.aa. per le proprie finalità istituzionali secondo le modalità di cui all'art. 58 del Cad, ai criteri per l'interoperabilità dell'Anpr con le altre banche dati di rilevanza nazionale e regionale e all'erogazione di altri servizi resi disponibili dall'Anpr (art. 62, comma 6). In sede di conversione è stato poi precisato che l'Anpr assicura al singolo comune la disponibilità dei dati anagrafici della popolazione residente per lo svolgimento delle funzioni di competenza statale attribuite al sindaco quale ufficiale del Governo, permettendo

ai medesimi comuni di autorizzarne l'utilizzo (anche con convenzioni) da parte di soggetti (non meglio identificati) aventi diritto. Inoltre, l'Anpr consente esclusivamente ai comuni la certificazione dei dati anagrafici ai sensi dell'art. 33 del d.P.R. n. 223/1989. La norma è stata integrata sulla base di una proposta parlamentare secondo cui tale base di dati è sottoposta ad un *audit* annuale di sicurezza in conformità alle regole tecniche dell'art. 51 del Cad, i cui risultati sono inseriti nella Relazione annuale del Garante (art. 62, comma 1). Il primo *audit* dovrebbe pertanto svolgersi nel 2013, e riguardare aspetti relativi alla sicurezza dei dati personali; si noti, peraltro, il rinvio all'art. 51 del codice dell'amministrazione digitale, che individua i parametri di controllo in termini relativamente ampli, rilevanti segnatamente sotto il profilo tecnico, quali la sicurezza dei sistemi e dei dati;

c) (Revisione della disciplina *privacy* in ambito statistico). L'art. 3, comma 4, demanda a un regolamento di delegificazione, emanato previo parere del Garante, il complessivo riordino del Sistema statistico nazionale, nel rispetto di alcuni parametri tra cui, in particolare, quello di "*adeguare alla normativa europea e alle raccomandazioni internazionali la disciplina in materia di tutela del segreto statistico, di protezione dei dati personali oggetto di trattamento per finalità statistiche, nonché di trattamento ed utilizzo dei dati amministrativi a fini statistici*" (comma 4). Con nota indirizzata al Presidente dell'Istat, il Garante ha recentemente assicurato la piena disponibilità a collaborare per i profili di competenza in vista dell'espressione del parere. Si novella inoltre il d.lgs. n. 322/1989, prevedendo, tra l'altro, la sostituzione integrale dell'art. 12, in base al quale la Commissione per la garanzia della qualità dell'informazione statistica contribuisce ad assicurare il rispetto della normativa in materia di segreto statistico e di protezione dei dati personali, garantendo sia al Presidente dell'Istat e al Garante la più ampia collaborazione, "*ove richiesta*"; sia che l'Autorità "*sentita ai fini della sottoscrizione dei codici di deontologia e di buona condotta relativi al trattamento dei dati personali nell'ambito del Sistema statistico nazionale*" (art. 3, comma 6);

d) (Domicilio digitale). L'art. 4 prevede -con l'inserimento nel Cad dell'art. 3-*bis*- che il cittadino possa indicare alla p.a., quale proprio domicilio digitale, una propria casella di posta elettronica certificata (Pec). L'indirizzo è inserito nell'Anpr così da renderlo disponibile a tutte le amministrazioni e ai gestori di pubblici servizi; un apposito decreto del

Ministro dell'interno, sentita l'Agenzia per l'Italia Digitale, dovrà definire le modalità di comunicazione, variazione e cancellazione del domicilio digitale da parte del cittadino, nonché le modalità di consultazione dell'Anpr da parte dei gestori ed esercenti di pubblici servizi per la ricerca del domicilio digitale degli utenti. A decorrere dal 1º gennaio 2013, le pp.aa. e i gestori o esercenti pubblici servizi comunicano con il cittadino solo attraverso il domicilio digitale; tuttavia, in assenza dello stesso, le pp.aa. possono predisporre le comunicazioni ai cittadini attraverso documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, conservate in archivi, e l'invio ai cittadini stessi, per posta ordinaria o raccomandata a.r., di copia analogica sottoscritta con firma autografa sostituita a mezzo stampa (art. 3 d.lgs. n. 39/1993);

e) (Indice nazionale degli indirizzi d'imprese e professionisti - Ini-Pec). L'art. 5 istituisce, presso il Ministero dello sviluppo economico, un Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (Ini-Pec), così consentendo alla pubblica amministrazione un accesso unico ai dati di tali soggetti, ai fini dell'invio di comunicazioni mediante Pec, che rappresenta il canale cui -salve diverse disposizioni normative- devono avvenire le comunicazioni tra imprese e pp.aa. (nuovo art. 6-*bis* del Cad). L'indice è realizzato sulla base degli elenchi di indirizzi Pec costituiti presso il registro delle imprese e gli ordini o collegi professionali. Un apposito decreto del predetto Ministero dovrà regolamentare, tra l'altro, le modalità di accesso e di aggiornamento dell'Indice. Con un emendamento parlamentare è stato specificato che l'accesso all'Ini-Pec è consentito non solo alle p.a., ai professionisti, alle imprese e ai gestori dei pubblici servizi, ma anche a tutti i cittadini, tramite sito web senza necessità di autenticazione. La norma va letta anche alla luce della recente esclusione delle "persone giuridiche" dalle garanzie in materia di protezione dei dati personali;

f) (Basi critiche). All'Agenzia per l'Italia Digitale è affidata la predisposizione delle regole tecniche per l'identificazione, tra le basi di dati di interesse nazionale definite dal Cad, delle basi critiche, precisando, al contempo, le modalità di aggiornamento (art. 2-*bis*);

g) (Archivio nazionale dei numeri civici delle strade urbane). Si prevede che con d.P.C.m. siano stabiliti i contenuti dell'Archivio nazionale dei numeri civici delle strade urbane

(Anncsu), le modalità di accesso all'archivio da parte dei soggetti autorizzati, nonché i criteri per la sua interoperabilità con le altre banche dati di rilevanza nazionale e regionale (art. 3, comma 2).

Nelle successive sezioni del provvedimento normativo si evidenziano le seguenti disposizioni:

h) (Trasmissione telematica di certificazioni di malattia). L'art. 7 estende alle categorie dei pubblici dipendenti sinora escluse le norme sulla trasmissione per via telematica delle certificazioni di malattia (ad eccezione delle forze armate) di cui all'art. 55-*septies* ("Controlli sulle assenze") del testo unico sul pubblico impiego. Inoltre, il medesimo articolo è integrato con la previsione che, su domanda del lavoratore, il medico o la struttura sanitaria invii telematicamente la certificazione all'indirizzo di posta elettronica (ordinaria) dello stesso (art. 7, commi 1 e 1-*bis*). Mediante una modifica dell'art. 47 del d.lgs. 26 marzo 2001, n. 151, recante "Testo unico delle disposizioni legislative in materia di tutela e di sostegno della maternità e della paternità a norma dell'art.15 della l. 8 marzo 2000, n. 53", si sostituisce altresì l'obbligo di presentazione al datore di lavoro della certificazione di malattia dei figli -ai fini della fruizione del relativo congedo da parte del lavoratore dipendente (anche nel settore privato)- con l'invio del certificato in via telematica da parte del medico stesso all'Inps, il quale l'inoltra immediatamente, sempre in via telematica, al datore interessato e all'indirizzo di posta elettronica del lavoratore che ne faccia richiesta (art. 7, comma 3). Un d.P.C.m. da adottarsi previo parere del Garante dovrà individuare le disposizioni necessarie per l'attuazione delle descritte norme, in conformità alle regole tecniche previste dal Cad (art. 7, comma 3-*bis*);

i) (Riutilizzo dei dati e "dati di tipo aperto"). L'art. 9, ai commi 1, lett. *a)*, 2 e 3, reca disposizioni in materia di riutilizzo di dati e di "dati di tipo aperto" (sostituzione integrale degli art. 52 e 68, comma 3, del Cad). In particolare, si dispone che i dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza, si intendono rilasciati come "dati di tipo aperto", dovendo intendersi per tali le informazioni che, tra l'altro, sono rese disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private. Si prevede altresì che le pp.aa. pubblichino nel sito web (sezione trasparenza) il catalogo dei

dati, dei metadati e delle relative banche dati in loro possesso, nonché i regolamenti disciplinanti l'esercizio della facoltà di accesso telematico e il riutilizzo, salvi i dati presenti in Anagrafe tributaria (art. 52, comma 1, Cad);

l) (Acquisizione di *software* da parte della p.a.). Nel modificare l'art. 68 del Cad si prevede che le pp.aa., prima di acquistare programmi informatici secondo le procedure del codice degli appalti, valutino le diverse soluzioni disponibili sul mercato alla luce di una serie di criteri tra cui le garanzie del fornitore in materia di livelli di sicurezza, nonché di conformità alla normativa in materia di protezione dei dati personali (art. 9-*bis*; art. 68, comma 1-*bis*, Cad);

m) (Fascicolo elettronico degli studenti). A partire dall'anno accademico 2013-2014 le università dovranno adottare il fascicolo elettronico dello studente contenente tutti i dati relativi alla carriera dello studente (art. 10, comma 1). Il fascicolo è alimentato dall'Anagrafe nazionale degli studenti di cui all'art. 3 del d.lgs. 15 aprile 2005, n. 76, e successive modificazioni, contenente anche i dati sugli iscritti alla scuola dell'infanzia (art. 10, comma 4); le università possono accedere, in modalità telematica, alle informazioni dell'Anagrafe nazionale degli studenti e dei laureati delle università di cui all'art. 1-*bis* del d.l. 9 maggio 2003, n. 105, convertito, con modificazioni, dalla l. 11 luglio 2003, n. 170 (art. 10, comma 5); al fine di evitare duplicazioni di banche dati contenenti informazioni similari, entrambe le predette anagrafi rappresentano banche dati a livello nazionale alle quali accedono anche le regioni e gli enti locali in relazione alle proprie competenze (art. 10, comma 8). Le università accedono altresì alle banche dati dell'Inps "*per la consultazione dell'indicatore della situazione economica equivalente (Isee) e degli altri dati necessari al calcolo dell'Indicatore della situazione economica equivalente per l'università - Iseeu*" (art. 10, comma 7);

n) (Fascicolo sanitario elettronico). L'art. 12 prevede l'istituzione, da parte delle regioni e delle province autonome, del fascicolo sanitario elettronico (fse) nel rispetto della normativa in materia di protezione dei dati personali. Si tratta di un istituto che ancora non era disciplinato a livello nazionale da norme di carattere primario o secondario, ma oggetto delle linee-guida di cui all'intesa tra il Governo, le regioni e le Province autonome di Trento e Bolzano, sancita dalla relativa conferenza permanente il 10 febbraio 2011. Si demanda a un decreto ministeriale, da emanarsi previo parere del Garante, la disciplina generale

dell'istituto. Il fse può essere alimentato esclusivamente sulla base del consenso libero e informato dell'assistito che decide quali dati sanitari non devono essere inseriti nel fascicolo medesimo (art. 12, comma 3-*bis*). Il decreto stabilirà, tra l'altro, i contenuti del fse, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, le modalità e i livelli diversificati di accesso al fse, la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato. Con disposizioni aggiunte dalla legge di conversione si è previsto che il fse deve consentire anche l'accesso del cittadino ai servizi sanitari *online*, secondo modalità determinate nel medesimo decreto (art. 12, comma 2, ultimo periodo). A tal fine, la consultazione dei dati e documenti presenti nel fse può essere realizzata soltanto in forma protetta e riservata e le interfacce, i sistemi e le applicazioni *software* adottati devono assicurare piena interoperabilità tra le soluzioni secondo modalità determinate dal decreto di cui al comma 7 (art. 12, comma 6-*bis*);

o) (Sistemi di sorveglianza e registri). L'art. 12 disciplina inoltre l'istituzione, a livello nazionale, di sistemi di sorveglianza nonché di registri di mortalità, di tumori, di altre patologie, di impianti protesici, di trattamenti costituiti da trapianti di cellule e tessuti e di trattamenti a base di medicinali per terapie avanzate o a base di prodotti di ingegneria tessutale. Essi sono istituiti nonché aggiornati periodicamente con d.P.C.m, acquisito il parere del Garante (art. 12, commi 10 e 11). La disciplina dell'accesso ai registri e della custodia e sicurezza dei dati è demandata a un regolamento governativo, da emanarsi su proposta del Ministro della salute e previo parere del Garante, e nel rispetto dei princìpi di pertinenza, indispensabilità, necessità di cui agli artt. 3, 11 e 22 del Codice (commi 13 e 14). Ulteriori registri possono essere istituiti, con legge, dalle regioni (o dalle province autonome) (comma 12);

p) (Prescrizione medica e cartella clinica digitale). L'art. 13 prevede la graduale sostituzione del formato cartaceo della prescrizione medica concernente farmaci o prestazioni specialistiche a carico del servizio sanitario nazionale con quello elettronico. La disposizione sancisce altresì che con decreto del Ministro della salute siano definite le modalità di attuazione della prescrizione medica digitale (art. 13, comma 2). Inoltre, attraverso una

modifica dell'art. 47-*bis* del d.l. 9 febbraio 2012, n. 5, convertito dalla l. 4 aprile 2012, n. 35, dal 1° gennaio 2013, la conservazione delle cartelle cliniche è effettuabile anche solo in forma digitale nel rispetto sia del Cad che del Codice (art. 13, comma 5);

q) (Traffico telematico). L'art. 14, comma 10-*bis,* aggiunge il comma 2-*bis* all'art. 6 del d.l. 27 luglio 2005, n. 144, convertito dalla l. 31 luglio 2005, n.155 prevedendo che gli utenti che attivino schede elettroniche (*sim*) abilitate al solo traffico telematico ovvero utilizzino postazioni pubbliche non vigilate o punti di accesso *wireless* ad internet "*possono essere identificati e registrati anche in via indiretta, attraverso sistemi di riconoscimento via sms e carte di pagamento nominative*". Con decreto del Ministro dell'interno, di concerto con il Ministro dello sviluppo economico, potranno essere previste misure di maggior dettaglio o ulteriori procedure semplificate;

r) (Pagamenti elettronici). L'art. 15 del decreto, sostituendo l'art. 5 del Cad, prevede per le pp.aa. e per i gestori di pubblici servizi l'obbligo di consentire agli utenti di pagare mediante carte di debito, di credito o prepagate, o tramite ulteriori strumenti di pagamento elettronico (art. 15, comma 1). In particolare, con decreto del Ministro dello sviluppo economico sarà disciplinata l'estensione delle modalità di pagamento effettuate anche avvalendosi di "tecnologie mobili" (art. 15, comma 2);

s) (Comunicazioni e notificazioni telematiche nel processo). L'art. 16 prevede che nei procedimenti civili e penali le comunicazioni e le notificazioni a cura della cancelleria (purché a persone diverse dall'imputato) dovranno essere effettuate esclusivamente per via telematica all'indirizzo di Pec risultante da pubblici elenchi o comunque accessibili alle pp.aa.. Si precisa poi -in linea con le indicazioni fornite dal Garante in sede di parere su precedenti decreti- che la notificazione o comunicazione che contiene dati sensibili è effettuata solo per estratto con contestuale messa a disposizione dell'interessato, sul sito internet individuato dall'amministrazione, dell'atto integrale, cui il destinatario accede mediante gli strumenti di cui all'art. 64 del Cad (art. 16, comma 5);

t) (Crisi da sovraindebitamento). L'art. 18 -recependo il contenuto di una precedente iniziativa del Governo- novella la l. 27 gennaio 2012, n. 3 recante disposizioni in materia di usura e di estorsione, che ha istituito procedure particolari per la composizione, da parte di

organismi ad *hoc* istituiti, delle cd. "crisi da sovraindebitamento". Le modifiche apportate concernono, fra l'altro, la prevista possibilità per il giudice e -su sua autorizzazione- per gli organismi di composizione della crisi di accedere a informazioni utili. In particolare il nuovo art. 15 della l., ai commi 10 e 11, prevede che gli organismi sopra indicati possano accedere ai dati contenuti nell'Anagrafe tributaria, nei sistemi di informazioni creditizie, nelle centrali rischi e nelle "altre banche dati pubbliche" (ivi compreso l'archivio centrale informatizzato di cui all'art. 30-*ter* del d.lgs. n. 141/2010 per la lotta alle frodi nel settore del credito al consumo mediante furto d'identità), in conformità al Codice e al codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti. La genericità dell'espressione *"altre banche dati pubbliche"* è temperata dal richiamo espresso al vincolo del rispetto alle norme del Codice contenuto nella stessa norma, per evitare l'accesso a informazioni non rilevanti. I dati personali sono trattati e conservati per i soli fini e tempi della procedura di composizione della crisi, e distrutti a termine della stessa procedura (art. 18, comma 1, lett. *t)*, del d.l.);

u) (Contrasto delle frodi assicurative). Si prevede che l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Ivass), da poco subentrato all'Isvap, curi la prevenzione delle frodi nel settore dell'assicurazione Rca, avvalendosi di un archivio informatico integrato connesso con una serie di banche dati (art. 21, commi 1 e 3); con decreto del Ministro dello sviluppo economico e del Ministro delle infrastrutture e dei trasporti, sentito il Garante, saranno stabilite poi le relative modalità di connessione delle banche dati, i termini, le modalità e le condizioni per la gestione e conservazione dell'archivio e per l'accesso al medesimo (art. 21, comma 3).

Condominio

4) La l. 11 dicembre 2012, n. 220, recante modifiche alla disciplina del condominio negli edifici (in G.U. 17 dicembre 2012, n. 293), reca alcune disposizioni rilevanti per la protezione dei dati personali e, in particolare, la disciplina delle delibere condominiali per l'installazione di impianti di videosorveglianza, di cui al nuovo art. 1122-*ter*, del codice civile (art. 7). La disposizione sancisce che "*le deliberazioni concernenti l'installazione sulle parti comuni dell'edificio di impianti volti a consentire la videosorveglianza su di esse sono approvate dall'assemblea con la maggioranza di cui al secondo comma dell'art. 1136*"; quest'ultima

disposizione, a sua volta, asserisce che "*sono valide le deliberazioni approvate con un numero di voti che rappresenti la maggioranza degli intervenuti e almeno la metà del valore dell'edificio*". Al riguardo il Garante aveva in due occasioni rappresentato agli organi competenti le ragioni per le quali appariva opportuno un intervento legislativo sull'argomento. Di interesse anche alcune disposizioni che impongono all'amministratore, ai sensi del novellato art. 1129 c.c. ("Nomina, revoca ed obblighi dell'amministratore"), di comunicare (ai condomini), tra l'altro, i propri dati anagrafici e professionali ed il codice fiscale, nonché di affiggere nel luogo di accesso al condominio o di maggior uso comune, accessibile anche a terzi, "*l'indicazione delle generalità, del domicilio e dei recapiti, anche telefonici…*" (art. 9 della legge); in base al nuovo art. 1130 c.c. ("Attribuzioni dell'amministratore") di curare la tenuta del registro di Anagrafe condominiale contenente anche le generalità dei singoli proprietari (e dei titolari di diritti reali e di diritti personali di godimento) comprensive del codice fiscale e della residenza o domicilio, del registro dei verbali delle assemblee, del registro di nomina e revoca dell'amministratore e del registro di contabilità (quest'ultimo anche con modalità informatizzate), conservando, al contempo, tutta la documentazione inerente alla gestione (art. 10 della legge); di "*comunicare ai creditori non ancora soddisfatti…i dati dei condomini morosi*" (art. 18 che sostituisce l'art. 63 disp. att. c.c. e disposizioni transitorie); e infine di attivare, su richiesta dell'assemblea, "*un sito internet del condominio che consenta agli aventi diritto di consultare ed estrarre copia in formato digitale dei documenti previsti dalla delibera assembleare*" (art. 25 che inserisce l'art. 71-*ter* nelle disp. att. c.c.).

Misure per la trasparenza dell'attività amministrativa

5) Nel 2012 si sono succeduti numerosi atti normativi in tema di trasparenza dell'azione amministrativa che, com'è noto, costituisce livello essenziale delle prestazioni concernenti diritti civili e sociali, ai sensi dell'art. 117, secondo comma, lettera *m)*, della Costituzione.

a) Al riguardo si rammentano, innanzitutto, le norme in materia di trasparenza confluite nella recente legge "anticorruzione" 6 novembre 2012, n. 190. L'art. 1, comma 15, stabilisce che la trasparenza dell'attività amministrativa è assicurata attraverso *"la pubblicazione, nei siti web istituzionali delle pubbliche amministrazioni, delle informazioni relative ai procedimenti amministrativi, secondo criteri di facile accessibilità, completezza e semplicità di consultazione, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio e di protezione dei*

dati personali". La legge individua tali procedimenti almeno in quelli di autorizzazione o concessione, scelta del contraente per affidamenti di lavori, forniture e servizi, concessioni ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari e attribuzione di qualsiasi vantaggio economico, concorsi e prove selettive per assunzione e progressione di carriera. È importante sottolineare che con uno o più decreti del Ministro per la pubblica amministrazione e la semplificazione dovranno essere individuate le informazioni rilevanti e le relative modalità di pubblicazione ai fini dell'applicazione delle disposizioni sulla trasparenza descritte. In occasione del parere sugli schemi di decreto, che dovrà essere richiesto ai sensi dell'art. 154, comma 4, del Codice, il Garante potrà formulare eventuali osservazioni per conformarne il contenuto ai princìpi e alle garanzie in materia di protezione dei dati personali;

b) (Riordino della disciplina in materia di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni). La l. n. 190/2012 ha poi delegato il Governo ad adottare un decreto legislativo per il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pp.aa., mediante la modifica o l'integrazione delle disposizioni vigenti, ovvero mediante la previsione di nuove forme di pubblicità (comma 35), nel rispetto di specifici princìpi e criteri direttivi;

c) altre disposizioni sulla trasparenza sono contenute nel d.l. 10 ottobre 2012, n. 174, recante disposizioni urgenti in materia di finanza e funzionamento degli enti territoriali, convertito dalla l. 7 dicembre 2012, n. 213.

In particolare:

- l'art. 3, ("Rafforzamento dei controlli in materia di enti locali"), interviene in materia di Anagrafe patrimoniale degli amministratori degli enti locali con più di 15.000 abitanti, introducendo nel d.lgs. 18 agosto 2000, n. 267, recante il testo unico delle leggi sull'ordinamento degli enti locali, l'art. 41-*bis*. Tale disposizione demanda ai regolamenti degli enti locali la disciplina delle modalità di pubblicità e trasparenza dello stato patrimoniale dei titolari di cariche elettive e di governo di loro competenza. La norma prevede che sia pubblicata annualmente sul sito internet, una dichiarazione contenente, tra l'altro, "*i dati di reddito e di patrimonio con particolare riferimento ai redditi annualmente dichiarati*";

- (Regioni) parallelamente a quanto prescritto dall'art. 3 per gli enti locali, la lettera *f)* del comma 1 dell'art. 2 della legge in esame prescrive alle regioni analoghi obblighi di pubblicità e trasparenza dello stato patrimoniale dei titolari delle cariche elettive e di governo; la norma va raccordata con le disposizioni della l. 5 luglio 1982, n. 441 (Disposizioni per la pubblicità della situazione patrimoniale di titolari di cariche elettive e di cariche direttive di alcuni enti), relativamente ai consiglieri regionali;

d) di rilievo è anche l'art. 18 ("Amministrazione aperta") del d.l. 22 giugno 2012, n. 83, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 134, in base al quale le amministrazioni pubbliche, le aziende speciali e le società "*in house*" sono tenute alla pubblicazione sul relativo sito internet, di tutte le informazioni concernenti la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e l'attribuzione dei compensi a persone, professionisti, imprese ed enti privati, prevedendosi altresì, dal 1° gennaio u.s. alla pubblicazione dei dati sul sito internet quale condizione legale di efficacia del titolo legittimante delle concessioni ed attribuzioni a imprese, professionisti e consulenti. Le informazioni sono riportate, con apposito *link* sulla pagina iniziale del sito, nel novero dei dati della sezione "Trasparenza, valutazione e merito", e devono risultare di agevole consultazione, nonché accessibili ai motori di ricerca e in formato tabellare aperto per consentirne l'esportazione, il trattamento e il riuso, ai sensi dell'art. 24 del Codice in materia di protezione dei dati personali;

e) infine, l'art. 4, d.l. sulla salute "cd. Balduzzi" modificando ulteriormente il d.lgs. 30 dicembre 1992, n. 502, introduce due disposizioni in materia di trasparenza dell'attività dei dirigenti sanitari. In particolare la regione assicura, anche mediante il proprio sito internet, adeguata pubblicità e trasparenza ai bandi, alla procedura di selezione, alle nomine e ai *curricula* per la nomina dei direttori generali delle aziende e degli enti del servizio sanitario regionale (art. 3-*bis*, comma 3, del d.l. 30 dicembre 1992, n. 502, come modificato dall'art. 4, lett. *a)*); inoltre, il profilo professionale del dirigente da incaricare nonché i *curricula* dei candidati sono pubblicati sul sito internet dell'azienda prima della nomina. Sono altresì pubblicate sul sito dell'ateneo e dell'azienda ospedaliero-universitaria interessati i *curricula* dei candidati e l'atto motivato di nomina (art. 15, comma 7-*bis* del d.l. 30 dicembre 1992, n. 502, introdotto dall'art. 4, lett. *d)*).

6) La l. 6 novembre 2012, n. 190, reca disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (in G.U. 13 novembre 2012, n. 265).

a) (Autorità nazionale anticorruzione). La legge prevede che la Commissione per la valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche (Civit) di cui all'art. 13 del d.lgs. 27 ottobre 2009, n. 150 (*infra,* Commissione), opera quale autorità nazionale anticorruzione svolgendo una serie di compiti tra cui quello di approvare il piano nazionale anticorruzione predisposto dal Dipartimento della funzione pubblica (art. 1, commi 1-3).

Fra le esigenze alla base del piano rileva particolarmente quella di monitorare i rapporti tra la p.a. e i soggetti contraenti o interessati a procedimenti di autorizzazione, concessione o erogazione di vantaggi economici di qualunque genere, *"anche verificando eventuali relazioni di parentela o affinità sussistenti tra i titolari, gli amministratori, i soci e i dipendenti degli stessi soggetti e i dirigenti e i dipendenti dell'amministrazione",* in termini che suscitano perplessità in relazione al principio di proporzionalità nel trattamento dei dati. Ulteriori dubbi suscita la previsione in base alla quale saranno individuati specifici obblighi di trasparenza, ulteriori rispetto a quelli previsti da disposizioni di legge;

b) (Segnalazione di illeciti cd. "*whistleblowing*"). Il comma 51 prevede l'inserimento nel d.lgs. n. 165/2001 dell'art. 54-*bis* ("Tutela del dipendente pubblico che segnala illeciti"), in base al quale il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria avente effetti sulle condizioni di lavoro per motivi collegati alla denuncia.

In caso di procedimento disciplinare, l'identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia invece fondata sulla segnalazione, l'identità può essere rivelata ove assolutamente indispensabile per la difesa dell'incolpato.

A tale riguardo, l'Aula della Camera ha approvato un ordine del giorno che impegna il Governo a monitorare gli effetti della disposizione, al fine di adottare "*ulteriori iniziative*

normative volte a prevedere che non sia resa pubblica l'identità della persona segnalante nel proprio ambito di lavoro, onde evitare possibili ripercussioni morali e fisiche di cui il segnalante potrebbe essere oggetto".

L'Autorità nel 2009 aveva segnalato al Parlamento e al Governo l'opportunità di un intervento normativo per disciplinare l'interferenza di tale fenomeno con le garanzie in materia di protezione dei dati personali, seppure con riferimento al settore privato. Rispetto alle indicazioni rese a suo tempo dal Garante, la norma appare poco dettagliata sulle fattispecie di possibile denuncia e sulla platea dei soggetti potenziali "segnalati" e non reca alcuna indicazione circa l'esercizio del diritto di accesso ai dati personali, ai sensi dell'art. 7 del Codice, da parte del "segnalato" con riguardo ai dati identificativi dell'autore della segnalazione. Si noti però che la legge sottrae la denuncia all'accesso ai documenti di cui alla l. n. 241/1990;

c) (Elenchi di soggetti per finalità di contrasto delle infiltrazioni mafiose cd. "*whitelist*"). Presso ogni prefettura è istituito l'elenco dei fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativo di infiltrazione mafiosa operanti nelle attività imprenditoriali maggiormente esposte al rischio di infiltrazione mafiosa. La prefettura effettua verifiche periodiche per accertare l'insussistenza dei suddetti rischi; al contempo, l'impresa comunica alla prefettura competente qualsiasi modifica dell'assetto proprietario e dei propri organi sociali (commi 52 e 55). Con d.P.C.m. sono definite le modalità per l'istituzione e l'aggiornamento dell'elenco nonché per l'attività di verifica (comma 56).

Salute

7) Il d.l. 13 settembre 2012, n. 158, convertito dalla l. 8 novembre 2012, n. 189, recante disposizioni urgenti per promuovere lo sviluppo del Paese mediante un più alto livello di tutela della salute (in G.U. 10 novembre 2012, n. 263) reca disposizioni di interesse in materia di ricetta elettronica, infrastruttura di rete regionale, tracciabilità dei pagamenti, monitoraggio dei dati relativi al rischio clinico. In particolare:

a) (Ricetta elettronica). L'art. 1, comma 4, apporta una serie di modifiche all'art. 8 del d.lgs. 30 dicembre 1992, n. 502 recante "Riordino della disciplina in materia sanitaria", prevedendo, in particolare, l'adesione obbligatoria dei medici all'assetto organizzativo e al sistema informativo definiti da ciascuna regione, nell'ambito del sistema informativo nazionale, compresi gli aspetti relativi al sistema della tessera sanitaria, nonché la parteci-

pazione attiva all'applicazione delle procedure di trasmissione telematica delle ricette mediche. Al riguardo, si rammenta che l'art. 20 ("Prescrizione medica e cartella clinica digitale") del d.l. 18 ottobre 2012, n. 179, recante "Ulteriori misure urgenti per la crescita del Paese", prevede la graduale sostituzione delle prescrizioni in formato cartaceo con le equivalenti in formato elettronico, dematerializzando la ricetta cartacea;

b) (Infrastruttura di rete e tracciabilità dei pagamenti). L'art. 2, apportando modifiche alla l. 3 agosto 2007, n. 120, recante "Disposizioni in materia di attività libero-professionale intramuraria e altre norme in materia sanitaria" prevede la predisposizione e attivazione, da parte delle regioni, di una infrastruttura di rete per il collegamento in voce o in dati, in condizioni di sicurezza, tra l'ente o l'azienda e le singole strutture nelle quali vengono erogate le prestazioni. In particolare, dovrà essere previsto, attraverso un utilizzo esclusivo della predetta infrastruttura, l'espletamento del servizio di prenotazione, la comunicazione, in tempo reale, da parte del professionista all'azienda sanitaria competente dei dati relativi all'impegno orario del sanitario, ai pazienti visitati, alle prescrizioni ed agli estremi dei pagamenti, anche in raccordo con le modalità di realizzazione del fascicolo sanitario elettronico. Le modalità tecniche per la realizzazione della infrastruttura saranno determinate con decreto, di natura non regolamentare, del Ministro della salute, nel rispetto del Codice (art. 1, comma 4, lett. a-*bis*, l. 3 agosto 2007, n. 120, come modificato dall'art. 2, lett. *c)*). Si prevede inoltre il pagamento di prestazioni di qualsiasi importo direttamente al competente ente o azienda del servizio sanitario nazionale, mediante mezzi di pagamento che assicurino la tracciabilità della corresponsione di qualsiasi importo.

Call center

8) Con un emendamento al d.l. 22 giugno 2012, n. 83, convertito dalla l. 7 agosto 2012, n. 134, recante misure urgenti per la crescita del Paese (cd. "Sviluppo") è stato inserito l'art. 24-*bis* recante misure a sostegno della tutela dei dati personali e dell'occupazione nelle attività svolte da *call center*. La norma prevede, fra l'altro, che quando un'azienda decide di spostare l'attività di *call center* fuori dal territorio nazionale (e le aziende già operanti in Paesi esteri), deve darne comunicazione al Ministero del lavoro nonché al Garante, indicando quali misure vengono adottate per il rispetto della legislazione nazionale, in particolare del Codice e del Registro delle opposizioni. Inoltre, è previsto che quando un cittadino effettua una

chiamata ad un *call center* deve essere informato preliminarmente sul Paese estero in cui l'operatore è fisicamente collocato, potendo scegliere che il servizio richiesto sia reso tramite un operatore collocato nel territorio nazionale; al contempo, se un cittadino è destinatario di una chiamata da un *call center*, deve essere preliminarmente informato sul Paese estero in cui l'operatore è fisicamente collocato.

La disposizione suscita perplessità, sul piano interpretativo e su quello applicativo, tanto che il Governo ha accettato presso le Commissioni 8ª e 10ª riunite del Senato, il 1° agosto, un ordine del giorno che lo impegna ad una ulteriore riflessione sulla materia.

Stampa

9) Il d.l. 18 maggio 2012, n. 63, convertito dalla l. 16 luglio 2012, n. 103, recante disposizioni urgenti in materia di vendita della stampa quotidiana e periodica, il cui art. 4, commi 4 e 5, autorizza i rivenditori di quotidiani e periodici a svolgere, in via telematica, attività connesse all'erogazione di servizi ai cittadini da parte delle p.a..

Al riguardo, il Garante, durante i lavori parlamentari, ha segnalato ai relatori e al rappresentante del Governo che non era espressamente previsto che il sistema informatico, del quale possono avvalersi i rivenditori, assicuri un adeguato livello di garanzie in termini di protezione dei dati personali. Inoltre, si riteneva necessario demandare a una norma di rango secondario la disciplina di attuazione di tale servizio, previa acquisizione del parere del Garante. In sede di approvazione del provvedimento da parte del Senato, il Governo si è impegnato a considerare i predetti rilievi nel d.P.C.m. attuativo del decreto-legge in esame.

Decreto-legge 24 gennaio 2012

10) il d.l. 24 gennaio 2012, n. 1, convertito con modificazioni dalla l. 24 marzo 2012, n. 27, disposizioni urgenti per la concorrenza, lo sviluppo delle infrastrutture e la competitività (cd. "liberalizzazioni" o "cresci Italia") (in G.U. 24 marzo 2012, n. 71) contiene alcune disposizioni d'interesse per l'Autorità anche in ragione del previsto coinvolgimento in sede di attuazione.

a) (Trasparenza sui mercati dell'energia elettrica e del gas). L'art. 22 prevede che il sistema informatico integrato per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica e del gas, istituito presso l'Acquirente Unico ai sensi dell'art. 1-*bis* del d.l. 8 luglio 2010, n. 105, sia finalizzato anche alla gestione delle informazioni relative ai consumi di energia elettrica e di gas dei clienti finali; conseguentemente, la relativa banca dati raccoglie,

oltre alle informazioni sui punti di prelievo ed ai dati identificativi dei clienti finali, anche i dati sulle relative misure dei consumi di energia elettrica e di gas. Si rammenta, in proposito, che ai sensi del predetto art. 1-*bis*, l'Autorità per l'energia elettrica e il gas (Aeeg) deve adottare specifici provvedimenti per la gestione dei flussi informativi e per il trattamento dei dati personali e sensibili, anche nel rispetto delle norme stabilite dal Garante.

In relazione alla collaborazione da tempo avviata tra il Garante e la predetta Autorità, si informa che è stato trasmesso alle Commissioni parlamentari competenti un documento dell'Aeeg recante indirizzi generali in tema di informazioni concernenti eventuali inadempimenti contrattuali dei clienti finali dei mercati dell'energia elettrica e del gas; le predette Commissioni di Camera e Senato si sono rispettivamente espresse con parere il 6 giugno ed il 16 maggio 2012;

b) (Repressione delle frodi nel settore assicurativo). L'art. 30 ("Repressione frodi"), prevede che le imprese assicurative esercitanti il ramo responsabilità civile per gli autoveicoli terrestri, trasmettano all'Isvap una relazione annuale contenente informazioni dettagliate sul numero dei sinistri oggetto di approfondimento in relazione al rischio di frodi, il numero delle querele o denunce presentate all'autorità giudiziaria, l'esito dei conseguenti procedimenti penali, nonché in ordine alle misure organizzative interne adottate o promosse per contrastare le frodi. Le medesime imprese pubblicano sui propri siti internet (o con altra idonea forma di diffusione) una stima relativa alla riduzione degli oneri per i sinistri derivante dall'accertamento delle frodi, conseguente all'attività di controllo e repressione delle frodi autonomamente svolta (comma 2). Nell'ambito del contrasto alla contraffazione dei contrassegni relativi ai contratti di assicurazione per la responsabilità civile verso i terzi per i danni derivanti dalla circolazione dei veicoli a motore su strada, l'art. 31 prevede che, con regolamento del Ministro dello sviluppo economico, siano definite le modalità per la progressiva dematerializzazione dei contrassegni, la loro sostituzione con sistemi elettronici o telematici, anche in collegamento con banche dati, le caratteristiche e i requisiti di tali sistemi e l'utilizzo, ai fini dei relativi controlli, dei dispositivi o mezzi tecnici di controllo e rilevamento a distanza delle violazioni del codice della strada (comma 1). A quest'ultimo proposito, il comma 3 precisa che la violazione dell'obbligo di assicurazione è rilevabile,

previa informativa agli automobilisti interessati, anche attraverso i dispositivi, le apparecchiature e i mezzi tecnici per il controllo del traffico e per il rilevamento a distanza delle violazioni delle norme di circolazione *ex* art. 45, comma 6, del codice della strada, i dispositivi e le apparecchiature per il controllo a distanza dell'accesso nelle zone a traffico limitato e altri sistemi per la registrazione del transito dei veicoli sulle autostrade o sulle strade sottoposte a pedaggio; con decreto del Ministro delle infrastrutture e dei trasporti, sentito anche il Garante, si dovranno definire le caratteristiche dei predetti sistemi di rilevamento a distanza, stabilendo, al contempo, le relative modalità di attuazione. La violazione è documentata con sistemi fotografici, di ripresa video o analoghi in grado di accertare i fatti costituenti illecito amministrativo, i dati di immatricolazione del veicolo ovvero il responsabile della circolazione, nel rispetto della esigenza di tutela della riservatezza.

Di rilievo è, infine, l'art. 32 ("Ispezione del veicolo, scatola nera, attestato di rischio, liquidazione dei danni") il quale, in particolare:

- aggiungendo un periodo al comma 1 dell'art. 132 ("Obbligo a contrarre") del codice delle assicurazioni private (d.lgs. 7 settembre 2005, n. 209), prevede che il consenso all'installazione di meccanismi elettronici che registrano l'attività del veicolo (cd. "scatola nera") o ulteriori dispositivi, permette all'assicurato di scaricare i relativi costi sulle compagnie che praticano, altresì, una riduzione tariffaria (comma 1). Inoltre, si prevedono un regolamento dell'Isvap, di concerto anche con il Garante, sulle modalità di raccolta, gestione e utilizzo dei dati raccolti dai predetti meccanismi elettronici, che definisca, al contempo, le modalità di interoperabilità degli stessi (comma 1-*bis*), e un decreto del Ministro dello sviluppo economico, sentito il Garante, con cui definire uno *standard* tecnologico comune *hardware* e *software*, per la raccolta, la gestione e l'utilizzo dei dati raccolti dai meccanismi in questione (comma 1-*ter*);

- al comma 3-*bis*, modificando l'art. 135 del codice delle assicurazioni private, prevede l'istituzione presso l'Isvap, accanto alla preesistente banca dati dei sinistri, di due banche dati denominate "Anagrafe testimoni" e "Anagrafe danneggiati"; il medesimo comma prevede, inoltre (mediante sostituzione del comma 3 dell'art. 135, che prima prevedeva un regolamento dell'Isvap secondo quanto previsto dall'art. 120 del Codice), che con

regolamento dell'Isvap, sentito anche il Garante, siano disciplinate le procedure di organizzazione e di funzionamento, le modalità e le condizioni di accesso alle banche dati suddette, da parte delle pp.aa., dell'autorità giudiziaria, delle forze di polizia, delle imprese di assicurazione e di soggetti terzi, nonché gli obblighi di consultazione delle stesse da parte delle imprese di assicurazione in fase di liquidazione dei sinistri.

2.2.2. Decreti legislativi

Sono stati infine adottati alcuni decreti legislativi d'interesse tra i quali si richiamano in particolare:

- d.lgs. 15 novembre 2012, n. 218, recante disposizioni integrative e correttive al d.lgs. 6 settembre 2011, n. 159, che disciplina il codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, cui si è fatto cenno nella Relazione 2011 (p. 45), che ha istituito la banca dati nazionale unica della documentazione antimafia presso il Ministero dell'interno (art. 96), specificando i dati in essa contenuti (art. 98) e i soggetti legittimati alla consultazione (art. 97). Le modalità di funzionamento della stessa sono demandate ad un regolamento, da adottarsi previo parere del Garante (art. 99), che non risulta allo stato essere stato ancora adottato. In particolare, l'art. 6 prevede disposizioni concernenti i collegamenti informatici o telematici utilizzabili in attesa della realizzazione della banca dati, sostituendo il comma 2-*bis* dell'art. 99 del predetto decreto legislativo del 2011, il quale stabilisce che fino all'attivazione della banca dati, e comunque non oltre dodici mesi dalla data di pubblicazione nella Gazzetta Ufficiale del primo dei regolamenti previsti, le pp.aa. e gli enti pubblici, gli enti e le aziende vigilati dallo Stato o da altro ente pubblico e le società o imprese comunque controllate dallo Stato o da altro ente pubblico nonché i concessionari di opere pubbliche e i contraenti generali, acquisiscono d'ufficio tramite le prefetture la documentazione antimafia. A tali fini, le prefetture utilizzano il collegamento informatico al Ced di cui all'art. 8 della l. 1° aprile 1981, n. 121;

- d.lgs. 19 settembre 2012, n. 169, recante ulteriori modifiche ed integrazioni al d.lgs. 13 agosto 2010, n. 141, recante attuazione della Direttiva n. 2008/48/CE, relativa ai contratti di credito ai consumatori, nonché modifiche nel settore finanziario e dei mediatori creditizi. Il

predetto decreto interviene sul sistema di prevenzione delle frodi nel settore del credito al consumo, con specifico riferimento al furto di identità, prevedendo che il Ministero dell'economia e delle finanze, titolare dell'archivio, possa avvalersi, per la gestione dell'archivio, di Consap, ente gestore, disciplinando con apposita convenzione i relativi rapporti;

- d.lgs. 30 maggio 2012, n. 85, recante modifiche ed integrazioni al d.lgs 25 gennaio 2010, n. 16, concernente l'attuazione delle Direttive nn. 2006/17/CE e 2006/86/CE, in materia di donazione, approvvigionamento e controllo di tessuti e cellule umani. Il Garante ha tenuto una audizione informale (28 marzo 2012) presso la Commissione affari sociali della Camera, competente ad esprimere il parere sullo schema di decreto, nel corso della quale sono state individuate criticità nel provvedimento normativo (cfr. *infra* par. 3.1.);

- d.lgs. 28 maggio 2012, n. 69, che, in attuazione della Direttiva n. 2009/136/CE recante modifica della Direttiva n. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, ha apportato significative modifiche al Codice (cfr. *supra* 2.1.3.).

3. Rapporti con il Parlamento e altre istituzioni

3.1. Le audizioni del Garante in Parlamento

Nel 2012 il Garante ha partecipato ad alcune audizioni presso commissioni parlamentari o altri organismi anche bicamerali su temi d'interesse all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge segnalando, nei diversi casi, i riflessi in materia di protezione dei dati personali.

In questo quadro si collocano:

a) il 29 marzo 2012, presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria, un'audizione nell'ambito dell'indagine conoscitiva sull'Anagrafe tributaria nella prospettiva del federalismo fiscale. In tale circostanza, il Garante si è soffermato, in particolare, sulle norme che prevedono l'accesso, da parte dei comuni, al casellario dell'assistenza presso l'Inps o alle banche dati dell'Anagrafe tributaria ovvero che prevedono la costituzione dell'Anagrafe immobiliare integrata. L'Autorità ha poi evidenziato la rilevanza del provvedimento del Direttore dell'Agenzia delle entrate concernente le modalità di comunicazione all'Anagrafe tributaria delle informazioni relative ai rapporti finanziari con la clientela sul quale il Garante ha reso un parere in data 17 aprile 2012 [doc. web n. 1886825] (cfr. *infra* 4.5.). Il documento conclusivo dell'indagine conoscitiva, approvato all'unanimità il 20 dicembre 2012, riporta il contributo reso dal Garante nell'audizione e, in particolare, nella sezione relativa alle garanzie ai contribuenti, un ampio riferimento all'accesso ai dati personali mediante una nuova classe di *web services*;

b) il 28 marzo 2012, presso la Commissione affari sociali della Camera dei deputati, un'audizione relativa allo schema di decreto legislativo recante modifiche al d.lgs. 25 gennaio 2010, n. 16, in materia di donazione, approvvigionamento e controllo di tessuti e cellule umani. Il Garante ha individuato alcune criticità rispetto alla comunicazione di dati inerenti le reazioni avverse verificatesi a seguito delle applicazioni sull'uomo, dal Centro nazionale trapianti (Cnt) al Registro delle strutture e dei nati con tecniche di procreazione medicalmente assistita (pma), istituito presso l'Istituto superiore di sanità. Il Garante ha osservato in particolare che è necessario assicurare che i dati relativi agli eventi o alle reazioni

avverse gravi, prima di essere inviati al Registro, siano già adeguatamente trattati in modo da non rendere identificabile l'interessato. Il Garante ha inoltre richiesto di perfezionare la disciplina del codice d'identificazione del materiale donato -atto a garantirne la tracciabilità- che individuava soltanto il contenuto minimo di tale codice, in termini che richiedevano maggiore chiarezza. Il d.lgs. 30 maggio 2012, n. 85, poi emanato, non ha però recepito le indicazioni rese dall' Autorità;

c) il 15 marzo 2012, presso la Commissione igiene e sanità del Senato, un'audizione nell'ambito dell'esame del disegno di legge recante delega al Governo per il riassetto della normativa in materia di sperimentazione clinica e disposizioni in materia sanitaria. Il Garante, in particolare, ha trattato della disciplina del fascicolo sanitario elettronico, dell'assistenza sanitaria *online,* nonché dei sistemi di sorveglianza e dei registri di patologia (la disciplina del fascicolo sanitario elettronico è poi confluita nel d.l. 18 ottobre 2012, n. 179, recante "Ulteriori misure urgenti per la crescita del Paese", convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221 (cfr. *supra* par. 2.2.1.).

3.2. L'AUTORITÀ E LE ATTIVITÀ DI SINDACATO ISPETTIVO E DI INDIRIZZO E CONTROLLO DEL PARLAMENTO

Nel 2012 l'Autorità ha fornito la consueta collaborazione al Governo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

In particolare, sono stati forniti elementi di valutazione ai fini della risposta, da parte del Governo, ai seguenti atti di sindacato ispettivo:

a) interrogazione n. 4-03212 concernente il trattamento di dati personali effettuato nell'ambito del servizio s*treet view* dalla società statunitense Google. L'Autorità ha riferito al Governo dei due provvedimenti (provv.ti 9 settembre 2010 [doc. web n. 1750529] e 15 ottobre 2010 [doc. web n. 1759972]) adottati al riguardo ed in particolare ha rammentato che nella fattispecie sono state applicate le norme del nostro ordinamento poiché il citato trattamento è effettuato con strumenti situati sul territorio italiano (cfr. art. 5, comma 2 del Codice) (nota 3 febbraio 2012);

b) interrogazioni n. 4-07386 e n. 4-03716 concernenti l'utilizzo delle risorse del Garante. L'Autorità ha precisato tra l'altro, che per i rimborsi spese dei componenti dell'organo collegiale si è evidenziato nel 2011 un decremento, anche se lieve; che il Garante non si avvale di consulenti ed ha anzi azzerato il relativo capitolo di bilancio, mentre, per altro verso, ha attuato una rigorosa revisione delle spese sia per le auto di servizio, sia per autolimitare le stesse spese di soggiorno e trasporto dei componenti residenti fuori Roma. Sono stati forniti ulteriori chiarimenti sul funzionamento del laboratorio *privacy* e su Civicrazia, coalizione associativa (note 29 maggio e 7 giugno 2012);

c) interrogazione a risposta immediata in assemblea n. 3-02465 concernente il Registro pubblico delle opposizioni, con la quale l'interrogante affermava che il Registro stesso si è rivelato "*strumento debole ed inefficace*", sia perché l'iscrizione è consentita alle sole utenze telefoniche oggetto di pubblicazione negli elenchi pubblici, che per il fatto che il consenso al trattamento dei propri dati personali per finalità commerciali, generalmente espresso dai cittadini in modo del tutto "inconsapevole", prevale sul dissenso eventualmente manifestato per il tramite dell'iscrizione nel Registro.

Con riferimento ai diversi profili evidenziati dall'interrogante, il Garante ha osservato che eventuali contatti indesiderati pervenuti su utenze non pubblicate in elenco derivano o dal mancato rispetto delle regole da parte di alcuni operatori (che contattano senza consenso numeri in realtà non contattabili), ovvero dalla circostanza che vengano sottoposti alla verifica presso il Registro delle opposizioni dati personali tratti da elenchi obsoleti, e non aggiornati; con ciò ricomprendendo anche utenze che abbiano nel tempo mutato la propria natura, passando da numeri inseriti in elenco a numeri riservati. Ha poi sottolineato che gli interessati che abbiano ricevuto una idonea informativa e manifestato nei confronti di un determinato titolare del trattamento un consenso specifico possono essere contattati da quel titolare per tali finalità anche nel caso in cui questi si iscrivano nel Registro, ferma restando la possibilità di opporsi successivamente (nota 11 settembre 2012).

Al riguardo, il 12 settembre 2012, nel fornire risposta all'interrogante, il Ministro per i rapporti con il Parlamento condivideva la necessità di individuare un punto di equilibrio tra i diversi interessi coinvolti, attraverso apposite iniziative normative che consentano di

includere nel Registro anche i numeri oggi non presenti negli elenchi telefonici pubblici, fatta salva la valutazione della fattibilità tecnica di questa proposta. Anche l'altra questione sulla prevalenza dell'iscrizione nel Registro rispetto ai consensi espressi singolarmente merita un adeguato approfondimento, seppure non possa negarsi, secondo il ministro interpellato, che rendere l'iscrizione al Registro in ogni caso prevalente su qualunque altro consenso fornito espressamente dall'interessato non gli consentirebbe di poter ricevere chiamate promozionali che lui stesso potrebbe avere consapevolmente autorizzato. Al riguardo, il Governo si è impegnato ad un'approfondita valutazione di tale questione al fine di individuare soluzioni adeguate che sappiano tutelare le scelte dei consumatori, confermando la disponibilità a tutte le iniziative dirette a rafforzare le garanzie dei cittadini con riguardo alle telefonate per scopi commerciali o per ricerche di mercato;

d) interrogazione a risposta immediata in assemblea n. 3-02557 concernente la delocalizzazione da parte di Telecom Italia dei servizi di *call center* all'estero. L'Autorità ha precisato di aver assunto diverse iniziative tese alla valutazione del fenomeno, effettuando accertamenti a carattere ispettivo e adottando provvedimenti, anche a carattere generale, in particolare rispetto a trattamenti di dati personali effettuati da soggetti che si avvalgono di agenti per attività promozionali, in tema di telefonate effettuate senza *calling line identification* e di telefonate "mute".

Inoltre, sulla base di specifiche disposizioni, (art. 24-*bis* d.l. n. 83/2012, convertito, con modificazioni dalla l. 7 agosto 2012, n. 134, che ha introdotto misure a sostegno della tutela dei dati personali, della sicurezza nazionale, della concorrenza e dell'occupazione nelle attività svolte da *call center* v. *supra* par. 2.2.), il Garante ha inviato ulteriori e dettagliate richieste di informazioni ai soggetti italiani maggiormente attivi nel settore del *telemarketing* (nota 24 ottobre 2012). Nel fornire risposta all'interrogante, il Ministro dello sviluppo economico e delle infrastrutture e dei trasporti non ha fatto riferimento a profili concernenti la protezione dei dati personali;

e) interrogazione n. 4-07537 concernente un articolo pubblicato su un quotidiano ad ampia tiratura relativo a conti correnti, operazioni bancarie ed investimenti dell'interrogante, sulla base di informazioni, a dire dell'interessata, divulgate da dipendenti dell'istituto bancario senza

alcuna autorizzazione e poi utilizzate dal giornalista per redigere un articolo ritenuto diffamatorio. L'Autorità ha informato di aver aperto un procedimento riservandosi ogni decisione in merito e ricordato di aver adottato tra l'altro un provvedimento generale in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (provv. 12 maggio 2011, in G.U. 3 giugno 2011, n. 127 [doc. web n. 1813953]), con il quale sono state prescritte ai titolari del trattamento una serie di misure, fra cui il tracciamento delle operazioni, la conservazione dei relativi *log*, l'implementazione di *alert* e un *audit* interno di controllo (nota 11 settembre 2012). Tutte le informazioni fornite dall'Autorità sono state riferite all'interrogante dal Sottosegretario di Stato per l'economia e le finanze il 7 gennaio 2013.

3.3. L'ATTIVITÀ CONSULTIVA DEL GARANTE SUGLI ATTI DEL GOVERNO

3.3.1. I pareri sugli atti regolamentari e amministrativi del Governo

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso anche nel 2012 diversi pareri i quali hanno riguardato, in particolare:

1) uno schema di decreto interministeriale concernente la sperimentazione finalizzata alla proroga del programma "carta acquisti", adottato ai sensi dell'art. 60 del d.l. n. 5 del 2012, convertito, con modificazioni, dalla l. n. 35/2012 (parere 6 dicembre 2012 [doc. web n. 2216848]). Il parere favorevole è stato reso su una versione del testo che teneva conto delle indicazioni ufficiose del Garante. Le osservazioni hanno riguardato, in particolare, l'individuazione dei tipi di dati e delle operazioni eseguibili, le modalità di realizzazione dei flussi informativi previsti tra i comuni e l'Inps, la definizione dei soggetti titolari e dei soggetti responsabili del trattamento in relazione alle varie fasi della sperimentazione, anche in riferimento all'articolazione su più livelli del trattamento, le garanzie a tutela degli interessati, anche in riferimento alle finalità di ricerca connesse alla valutazione della sperimentazione, e le misure di sicurezza;

2) uno schema di decreto del Presidente del Consiglio dei ministri in materia di consegna, da parte delle aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e

altre modalità digitali, nonché di effettuazione del pagamento *online* delle prestazioni erogate (parere 6 dicembre 2012 [doc. web n. 2223206]). Anche in questo caso, il testo già recepiva la gran parte delle indicazioni fornite dall'Ufficio, con particolare riferimento alle misure di sicurezza da adottarsi a cura delle aziende sanitarie, anche in relazione a quanto previsto dal Garante nelle linee-guida in tema di referti *online*. Nel parere favorevole il Garante ha inserito due osservazioni volte a chiarire che la refertazione *online* non può riguardare i referti relativi ad analisi genetiche e a sancire limiti e garanzie specifici per la fornitura dei referti relativi ad accertamenti di infezione da HIV;

3) uno schema di decreto del Presidente del Consiglio dei ministri recante il regolamento per la revisione delle modalità di determinazione e i campi di applicazione dell'indicatore della situazione economica equivalente (Isee) (parere 22 novembre 2012 [doc. web n. 2174496]). Il testo teneva conto dei suggerimenti forniti dall'Autorità, in particolare per quanto riguarda l'ambito soggettivo di applicazione delle disposizioni in esame, la pertinenza e non eccedenza dei dati trattati, le misure di sicurezza nella raccolta e nella trasmissione dei dati, i limiti e le condizioni relative al trattamento dei dati nell'ambito del sistema informativo Isee da parte dei centri di assistenza fiscale e degli enti erogatori;

4) uno schema di provvedimento del Direttore generale per gli italiani all'estero in materia di passaporto elettronico (parere 22 novembre 2012 [doc. web n. 2222980]). Il Garante ha reso parere favorevole sul testo, che prevede specifiche garanzie di sicurezza nella raccolta e nella trasmissione dei dati biometrici e nel loro inserimento nel *chip* collocato all'interno del "documento elettronico", l'obbligo di cancellazione delle impronte digitali al momento del rilascio del passaporto ed adeguate cautele per evitare abusi anche nell'ambito delle attività di controllo dell'autenticità dei dati riportati nel documento;

5) uno schema di regolamento del Ministro dell'economia e delle finanze concernente l'uso degli strumenti informatici e telematici nell'ambito del processo tributario in attuazione delle disposizioni contenute nell'art. 39, comma 8, lett. *d)*, del d.l. 6 luglio 2011, n. 98, convertito, con modificazioni, dalla l. 15 luglio 2011, n. 111 (parere 8 novembre 2012 [doc. web n. 2185215]). Gran parte delle procedure disciplinate in questo regolamento (si pensi alle notificazioni e alle comunicazioni in via telematica) sono analoghe a quelle proprie dei

procedimenti civile e penale telematici, come regolate dal decreto del Ministro della giustizia n. 44 del 2011 -"Regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione"- su cui il Garante aveva reso articolato parere (parere 21 dicembre 2011 [doc. web n. 1870802] v. Relazione 2011 p. 16). Il Garante ha richiesto che alcune cautele previste in quel decreto a tutela della riservatezza dei dati personali fossero osservate anche nel decreto in parola, in particolare per quanto riguarda la limitazione (soggettiva e oggettiva) degli accessi ai procedimenti tributari, in ossequio ai princìpi di pertinenza e non eccedenza dei dati e le particolari cautele da adottare per assicurare una tutela rafforzata ai dati sensibili;

6) uno schema di decreto del Ministro dell'interno riguardante modifiche al decreto ministeriale 11 dicembre 2000, recante "Disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive"(parere 18 ottobre 2012 [doc. web n. 2099252]). Il parere è stato favorevole in quanto reso su un testo che, nel recepire i suggerimenti forniti al Ministero, prevedeva idonee garanzie sulla selettività degli accessi, sugli *standard* di sicurezza nella trasmissione dei dati e sull'obbligo di cancellazione degli stessi dopo il decorso di un termine congruo;

7) uno schema di decreto dirigenziale *ex* art. 39 del d.P.R. n. 313/2002, recante il testo unico del casellario giudiziale, relativo alla consultazione diretta del Sistema informativo del Casellario da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi (parere 11 ottobre 2012 [doc. web n. 2091248]). Il testo ha ricevuto parere favorevole poiché teneva conto delle indicazioni del Garante relative, in particolare, alle modalità tecniche necessarie per garantire un accesso selettivo ai soli dati giudiziari indispensabili per lo svolgimento degli accertamenti di competenza, alla previsione di schemi-tipo di convenzione, per ambiti omogenei di attività, per l'accesso delle pp.aa. al sistema, da sottoporre a parere del Garante, nonché all'adeguatezza delle misure di sicurezza previste, per evitare accessi abusivi;

8) uno schema di decreto del Ministro dell'economia e delle finanze in materia di trasmissione per via telematica dei dati e delle informazioni relativi al ritiro dalla circolazione di banconote e monete metalliche in euro sospette di falsità (parere 4 ottobre 2012 [doc. web

n. 2067279]). Il parere è stato favorevole in quanto lo schema prevedeva, tra l'altro, idonee modalità tecniche di autenticazione del gestore del contante ai fini dell'invio delle previste informazioni al Mef/Dipartimento del tesoro, indicato come titolare del trattamento dei dati, tramite l'apposito sistema informativo (Sirfe);

9) uno schema di determina del Ragioniere generale dello Stato concernente le modalità di trasmissione (mediante utilizzo delle tecnologie dell'informazione e della comunicazione) e gestione di dati e comunicazioni ai Registri dei revisori legali dei conti annuali e dei conti consolidati (parere 20 settembre 2012 [doc. web n. 2068734]), istituiti in attuazione della Direttiva europea n. 2006/43/CE e del d.lgs. 27 gennaio 2010, n. 39 (sui regolamenti attuativi del d.lgs. il Garante aveva reso motivati pareri in data 10 novembre 2011 [doc. web n. 1851797]). Il parere è stato favorevole, in quanto lo schema specificava le finalità perseguite dal Ministero nella materia in esame; richiamava espressamente le ipotesi di cancellazione dei dati previste dai citati regolamenti ministeriali attuativi del d.lgs. n. 39/2010; specificava la figura del titolare del trattamento nel Ministero dell'economia e delle finanze-Dipartimento della Ragioneria Generale dello Stato e, infine, indicava puntuali misure di sicurezza, esplicitate nell'allegato tecnico;

10) uno schema di regolamento del Ministro degli affari esteri (Mae) recante disciplina dell'elenco dei funzionari internazionali di cittadinanza italiana, *ex* art. 2, comma 7, della l. 17 dicembre 2010, n. 227 (parere 26 luglio 2012 [doc. web n. 1922974]). In particolare, il regolamento impone la pubblicazione *online* sul sito del Mae relativamente a ciascun funzionario presente nell'elenco, di dati personali (di natura prettamente curriculare) selezionati in maniera pertinente e funzionale rispetto alla finalità di illustrare le competenze di ciascun funzionario e favorirne la mobilità. Il parere è stato pertanto favorevole, anche in questo caso;

11) uno schema di decreto del Presidente del Consiglio dei ministri concernente le modalità di attuazione del Regolamento (UE) n. 211 del 16 febbraio 2011 del Parlamento europeo e del Consiglio riguardante "l'iniziativa dei cittadini"(parere 19 luglio 2012 [doc. web n. 1919810]). Tale regolamento definisce "iniziativa dei cittadini" quella avente il sostegno di almeno un milione di firmatari appartenenti ad almeno un quarto degli Stati

membri dell'UE. Lo schema disciplina, tra l'altro, la regolamentazione della procedura per la presentazione delle dichiarazioni di sostegno e la loro verifica. In relazione a quest'ultimo aspetto, lo schema imponeva, tra l'altro, al Ministero dell'interno di procedere a un controllo a campione volto ad accertare la ricevibilità delle dichiarazioni di sostegno, la completezza dei dati richiesti per identificare il firmatario e la veridicità delle predette dichiarazioni, mediante raffronto tra i dati indicati nelle dichiarazioni e i dati detenuti dagli archivi anagrafici comunali o dalle questure (limitatamente ai dichiaranti che abbiano utilizzato il passaporto quale documento identificativo). Lo schema prevedeva che in assenza di riscontro al Ministero dell'interno entro 30 gg. "*la verifica dei dati contenuti nella dichiarazione di sostegno si intendesse favorevolmente accertata*". Al riguardo il Garante ha reso parere condizionato alla previsione di una procedura di verifica conforme all'art. 8 del suddetto Regolamento europeo n. 211 che richiede "*adeguati controlli*" e alle disposizioni dell'art. 11 del Codice, chiedendo di espungere dallo schema di regolamento ogni riferimento a sistemi di verifica solo formale della veridicità delle dichiarazioni stesse. Tale condizione non è stata però recepita nel testo approvato (d.P.R. 18 ottobre 2012, n. 193);

12) uno schema di ordinanza della Presidenza del Consiglio dei ministri - Dipartimento della protezione civile, emanata ai sensi dell'art. 5 della l. 24 febbraio 1992, n. 225, recante "Disposizioni urgenti dirette a fronteggiare gli eventi sismici verificatisi recentemente nella Regione Emilia Romagna" (parere 12 luglio 2012 [doc. web n. 1913546]). Il testo risultava conforme a quelli emanati in analoghe occasioni (terremoto in Abruzzo del 2009 e afflusso dei cittadini nordafricani nel 2011) sui quali il Garante si era espresso favorevolmente. Nel merito, il regime derogatorio in materia di protezione dati disposto dall'ordinanza sanciva un ragionevole bilanciamento con gli interessi costituzionalmente rilevanti all'efficacia delle operazioni di soccorso. Risultava comunque apprezzabile la previsione di un termine certo e determinato per la sospensione dell'efficacia delle norme del Codice sull'informativa, sulla designazione degli incaricati e sulle misure di sicurezza. Il parere del Garante è stato perciò favorevole;

13) uno schema di regolamento sul fondo per le vittime della mafia dell'usura e dell'estorsione (parere 5 luglio 2012 [doc. web n. 1913538]). In relazione a tale schema il

Garante ha espresso parere favorevole subordinatamente alla previsione di termini di conservazione dei dati proporzionati e non eccedenti rispetto alle esigenze cui il decreto stesso è preordinato, nonché di adeguate forme di tracciabilità degli accessi, necessariamente selettivi, agli archivi nei quali i dati personali trattati sono conservati, al fine di evitare possibili consultazioni abusive. Infine, l'Autorità ha fatto osservare all'Amministrazione l'opportunità di adottare un più ampio richiamo alle disposizioni del Codice;

14) uno schema di decreto del Ministro dell'istruzione, dell'università e della ricerca, riguardante le modalità e i contenuti delle prove di ammissione ai corsi di laurea e di laurea magistrale programmati a livello nazionale per l'anno accademico 2012-2013 (parere 28 giugno 2012 [doc. web n. 1912937]). Sullo schema di decreto, che nella sostanza riproduceva quello relativo all'anno accademico 2011/2012, il Garante ha espresso parere favorevole;

15) uno schema di decreto del Ministro dell'interno sulle regole tecniche per il permesso di soggiorno elettronico (parere 5 giugno 2012 [doc. web n. 1908393]). Nella fase preparatoria l'Ufficio ha espresso l'esigenza di precisare l'ambito soggettivo di applicazione delle disposizioni del decreto, con particolare riguardo alle varie tipologie di permesso di soggiorno, disciplinando adeguatamente il trattamento dei dati biometrici, nonché i termini e le modalità di conservazione dei dati personali dei titolari dei menzionati permessi nell'archivio informatizzato appositamente previsto, conformemente ai princìpi di proporzionalità, finalità e pertinenza; è stata richiamata altresì la necessità di prevedere adeguate cautele per evitare abusi anche nell'ambito delle attività di verifica e controllo dell'autenticità dei dati riportati nel documento. Il parere del Garante è stato favorevole con la raccomandazione all'Amministrazione di inserire nello schema di decreto una norma volta a individuare più idoneamente la disciplina applicabile, chiarendo espressamente il rapporto tra lo schema di decreto e quello precedente del 2008;

16) quattro schemi di decreto del Ministro della salute concernenti sistemi informativi in materia sanitaria, e in particolare: uno schema di decreto di modifica del d.m. 17 dicembre 2008 sulla banca dati per la rilevazione delle prestazioni residenziali e semiresidenziali (parere 17 aprile 2012 [doc. web n. 1907937]); uno schema di decreto di modifica del

d.m. del 31 luglio 2007 in materia di istituzione del flusso informativo delle prestazioni farmaceutiche (parere 11 maggio 2012 [doc. web n. 1900890]); uno schema di decreto di modifica del d.m. 17 dicembre 2008 sul sistema informativo di monitoraggio dell'assistenza domiciliare (parere 29 marzo 2012 [doc. web n. 1893476]); uno schema di decreto di modifica del d.m. 17 dicembre 2008 sul sistema informativo di monitoraggio delle prestazioni rese in emergenza-urgenza (parere 21 marzo 2012 [doc. web n. 1892560]). Poiché i testi erano sostanzialmente analoghi, il Garante li ha esaminati congiuntamente, formulando indicazioni riferibili a ciascuno di essi. In particolare, quanto all'identificazione dell'assistito, l'Autorità, nel rilevare che i provvedimenti, pur sancendo il carattere non direttamente identificativo dei dati trasmessi alla banca dati, di contro menzionavano anche i "dati anagrafici della persona", ha ritenuto necessaria la soppressione di tale ultimo riferimento; in secondo luogo, ha richiesto una più precisa indicazione delle finalità del trattamento; per i profili attinenti alle tecniche di archiviazione, ricerca e accesso alle informazioni rese disponibili dalla banca dati medesima, il Garante ha evidenziato l'obbligo di trattare con tecniche crittografiche i dati relativi alla patologia dell'interessato, al fine di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi; in ordine al disciplinare tecnico, allegato al decreto, il Garante ha richiesto, tra l'altro, l'eliminazione di alcune voci eccedenti rispetto alle finalità cui il monitoraggio è preordinato e, soprattutto, suscettibili di identificare, sia pure indirettamente, l'interessato; il Garante ha poi raccomandato all'Amministrazione di valutare l'opportunità di sviluppare i riferimenti a determinate voci, le quali rischiavano di rivelare informazioni per le quali la legge impone particolari cautele o dati comunque meritevoli di una tutela particolare; infine, in un caso l'Autorità ha ritenuto opportuna la previsione di accorgimenti, a garanzia della sicurezza dei dati riguardanti le prestazioni erogate, qualora la loro archiviazione e relativa trasmissione avvenga presso il domicilio dell'assistito.

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità in relazione a provvedimenti che -ancorché, non prevedano specifiche disposizioni in materia di protezione dei dati personali- incidono, in ogni caso, su tale materia.

In particolare si richiamano:

1) il decreto del Ministro dell'economia e delle finanze 24 dicembre 2012 (in G.U. 4 gennaio 2013, n. 3) recante il contenuto induttivo degli elementi indicativi di capacità contributiva sulla base dei quali può essere fondata la determinazione sintetica del reddito (cd. "redditometro");

2) il d.P.C.m. 14 novembre 2012, n. 252, recante i criteri e le modalità per la pubblicazione degli atti e degli allegati elenchi degli oneri introdotti ed eliminati, ai sensi dell'art. 7, comma 2, l. 11 novembre 2011, n. 180 "Norme per la tutela della libertà d'impresa. Statuto delle imprese";

3) il decreto del Ministro dell'economia e delle finanze 24 settembre 2012 (in G.U. 29 ottobre 2012, n. 253) concernente la determinazione dell'entità e delle modalità di versamento del contributo annuale degli iscritti al registro dei revisori legali;

4) il decreto del Ministro dell'economia e delle finanze, in qualità di Presidente del comitato interministeriale per il credito e il risparmio, 11 luglio 2012 (in G.U. 27 luglio 2012, n. 174), recante disciplina della Centrale dei rischi;

5) il d.P.C.m. 10 luglio 2012 (in G.U. 28 luglio 2012, n. 175), recante criteri e modalità per la pubblicazione, sul sito del comune, dei dati aggregati relativi alle dichiarazioni dei redditi e per la messa a disposizione di ulteriori dati al fine di favorire la partecipazione all'attività di accertamento nonché modalità di trasmissione idonee a garantire la necessaria riservatezza;

6) il decreto del Ministro della salute 9 luglio 2012 (in G.U. 26 luglio 2012, n. 173), recante contenuti e modalità di trasmissione delle informazioni relative ai dati aggregati sanitari e di rischio dei lavoratori, ai sensi dell'art. 40 del d.lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;

7) il decreto del Ministro dell'economia e delle finanze 4 maggio 2012 (in G.U. 12 maggio 2012, n. 110), in materia di segnalazione da parte del Consiglio nazionale dell'ordine dei dottori commercialisti di operazioni sospette di riciclaggio, recante attuazione dell'art. 43, comma 2, del d.lgs. 21 novembre 2007, n. 231;

8) il decreto del Direttore generale delle finanze 26 aprile 2012 (in G.U. 3 maggio 2012, n. 102), recante regole tecniche per l'utilizzo, nell'ambito del processo tributario, della posta

elettronica certificata (Pec), per le comunicazioni di cui all'art. 16, comma 1-*bis*, del d.lgs. n. 546 del 31 dicembre 1992;

9) il decreto del Ministro della salute 18 aprile 2012 (in G.U. 4 giugno 2012, n. 128), di modifica al decreto 26 febbraio 2012, recante definizione delle modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al sistema di accoglienza centrale.

3.3.2. Altri pareri

Il Garante ha formulato parere, su espressa richiesta del Governo, anche su altri atti normativi, aventi rango primario.

a) In particolare, ha reso parere sullo schema di disegno di legge concernente "Ratifica ed esecuzione dell'Accordo tra la Repubblica italiana e lo Stato di Israele sulla previdenza sociale, fatto a Gerusalemme il 2 febbraio 2010"(parere 25 ottobre 2012 [doc. web n. 2185056]).

L'accordo mira a garantire ai cittadini italiani che hanno lavorato in Italia prima di trasferirsi in Israele la possibilità di percepire direttamente in quel Paese un trattamento pensionistico in linea con i contributi versati in Italia. Nell'ambito della cooperazione amministrativa (art. 18) è previsto, tra l'altro, che su richiesta italiana, le autorità e le istituzioni israeliane competenti comunichino i dati necessari e le informazioni per la realizzazione del principio di parità di trattamento, che nella specie, per quanto concerne l'Italia, si riferisce ai cittadini dell'Unione europea.

L'attuazione dell'accordo presuppone dunque una comunicazione di dati personali da parte di un soggetto pubblico nazionale (il Ministero del lavoro e delle politiche sociali) ad altro soggetto (pubblico) straniero (e viceversa).

L'art. 44, comma 1, lett. *b)*, del Codice subordina il trasferimento di dati personali in Paesi non europei alla previa autorizzazione del Garante, resa in base ad adeguate garanzie per i diritti dell'interessato che si presumono sussistenti, tra l'altro, in presenza di una delle decisioni previste dagli artt. 25, paragrafo 6, e 26, paragrafo 4, della Direttiva n. 95/46/CE, con le quali la Commissione europea constata che il Paese in questione (non appartenente all'Unione europea) garantisce un livello di protezione adeguato (cd. "*adequacy decisions*").

Con Decisione 31 gennaio 2011 n. 2011/61/UE, la Commissione europea ha ritenuto che lo Stato d'Israele, come definito ai sensi del diritto internazionale, fornisca un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea per quanto attiene ai trasferimenti internazionali automatizzati di dati personali dall'Unione europea e, in caso di trasferimenti non automatizzati, ai dati che siano sottoposti a ulteriore trattamento automatizzato nello Stato d'Israele, perché la legge israeliana sulla protezione della vita privata si applica solo ai trattamenti automatizzati e non anche al trattamento di dati contenuti in banche dati "manuali" (considerando n. 9). Di conseguenza, il Gruppo Art. 29, nell'esprimere un parere sul livello di adeguatezza della protezione dei dati in quel Paese (*adequacy opinion*), ha auspicato l'estensione alle banche dati cartacee della normativa sulla protezione dati. Pertanto il Garante, il 20 gennaio 2012, ha autorizzato *ex* art. 44, comma 1, lett. *b)*, del Codice, i trasferimenti di dati personali dal territorio dello Stato verso lo Stato d'Israele, in conformità alla suddetta decisione e nei limiti da essa previsti, riservandosi, in conformità alla normativa comunitaria, al Codice e all'art. 3 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento.

I limiti che caratterizzano la predetta decisione della Commissione UE si riflettono anche sul parere allo schema di disegno di legge, e l'esecuzione dell'accordo non potrà che essere soggetta a un limite implicito, sul quale il Garante ha richiamato l'attenzione del Governo, ai fini del rispetto della Decisione della Commissione europea n. 2011/61/UE;

b) su richiesta del Ministro dello sviluppo economico e delle infrastrutture e dei trasporti, il Garante ha espresso parere sullo schema di d.lgs. di recepimento della Direttiva n. 2009/136/CE sulla tutela della vita privata nel settore delle comunicazioni elettroniche (parere 29 marzo 2012 [doc. web n. 1893400]), adottato ai sensi dell'art. 9 della l. 15 dicembre 2011, n. 217 (legge comunitaria 2010) e predisposto all'esito dei lavori di un apposito tavolo tecnico cui ha fornito il proprio contributo anche l'Ufficio del Garante (rinvio alle disposizioni del Codice; v. *supra* par. 2.2.).

3.4. I PARERI SULLE LEGGI REGIONALI

Nel 2012 è proseguita l'attività di esame e valutazione delle leggi regionali approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione (v. *infra* par. 22.7.).

Nella gran parte dei casi sottoposti all'attenzione dell'Autorità (18) è stato riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale rispetto ai profili di protezione dei dati personali.

Solo in un caso l'Autorità ha fornito alla Presidenza del Consiglio dei ministri osservazioni in merito alla compatibilità della legge con le disposizioni in materia di protezione dei dati personali -assunte quali norme interposte ai fini del sindacato di costituzionalità- quali elementi utili per la valutazione in ordine all'eventuale sussistenza dei presupposti necessari all'impugnazione della legge regionale. Si tratta della legge della Regione Emilia Romagna del 30 marzo 2012, n. 1, in materia di "Anagrafe pubblica degli eletti e dei nominati, disposizioni sulla trasparenza e l'informazione".

In particolare, l'art. 3 della legge prevede, in aggiunta a quanto disposto dalla l. n. 441/1982, la pubblicazione in internet di taluni dati personali inerenti la situazione patrimoniale, la formazione e l'attività istituzionale dei componenti l'Assemblea legislativa e la Giunta regionale, nonché del Presidente della Regione, e richiama tra i dati da pubblicare, tra gli altri, il codice fiscale, la "dichiarazione dei redditi e della situazione patrimoniale, così come espressamente previste dalla l. n. 441/1982, nonché dei conviventi *more uxorio* se gli stessi vi consentono", mentre la legge ora richiamata prevede la pubblicazione delle sole *"notizie risultanti dal quadro riepilogativo della dichiarazione dei redditi"* (art. 9, comma 1, l. n. 441/1982).

In tal modo, la legge regionale potrebbe legittimare la diffusione di dati -contenuti nelle dichiarazioni dei redditi- non strettamente pertinenti rispetto alle finalità della legge, con il rischio, dunque, di rivelare anche taluni dati sensibili, in violazione dell'art. 22, comma 8, del Codice e ciò, ovviamente, per i soli soggetti cui si riferisce la legge regionale in esame.

Analoghe perplessità l'Autorità ha espresso rispetto alle disposizioni della legge che impongono la pubblicazione di dati (si pensi al codice fiscale e alle dichiarazioni relative ai

finanziamenti) che appaiono non del tutto conferenti rispetto alla *ratio* stessa dell'istituto dell'Anagrafe patrimoniale, concepito quale espressione del rapporto di rappresentanza e del controllo democratico, da parte dei cittadini, in ordine alle attività e alle condizioni soggettive degli eletti rilevanti ai fini dell'esercizio del mandato.

L'Autorità ha, in conclusione, segnalato alla Presidenza del Consiglio che, in ragione del rilevato contrasto con le citate disposizioni del Codice (artt. 11 e 22, comma 8), assunte quali norme interposte ai fini del sindacato di costituzionalità, l'art. 3, comma 1, della legge è apparso incompatibile con il riparto di attribuzioni sancito dall'art. 117, secondo comma, lettera *l)* della Costituzione, eccedendo la competenza riservata al legislatore regionale, surrettiziamente disciplinando -con modalità diverse e incompatibili con quelle previste dal Codice- una materia, quale quella del trattamento dei dati personali, riservata alla potestà legislativa esclusiva dello Stato, in quanto riconducibile alla materia dell'ordinamento civile di cui all'art. 117, comma secondo, lettera *l)*, della Costituzione, giusta il principio sancito dalla Consulta con la sentenza n. 271/2005.

L'attività svolta dal Garante

II. L'attività svolta dal Garante

4. Il Garante e le pubbliche amministrazioni

4.1. I regolamenti sui trattamenti di dati sensibili e giudiziari

Il Garante, su richiesta della Regione Veneto ha espresso parere su uno schema di regolamento recante norme per il funzionamento del Registro dei tumori in attuazione della l.r. 16 febbraio 2010 n. 11 che prevede l'istituzione di diversi registri di interesse sanitario (provv. 13 settembre 2012 [doc. web n. 1927415]).

Il regolamento individua il titolare del trattamento, gli specifici scopi scientifici perseguiti, i tipi di dati sensibili trattati, i soggetti tenuti ad alimentare il Registro, nonché l'ambito di comunicazione e di diffusione dei dati ivi contenuti (art. 18, comma 2, l.r. 11/2010 cit. e artt. 20 e 98 del Codice).

Il Registro mira a raccogliere dati per consentire la ricerca scientifica e, in particolare, per descrivere l'incidenza dei tumori, le cause, la mortalità e i trattamenti più efficaci, anche mediante studi epidemiologici.

Il testo tiene conto delle indicazioni fornite in via ufficiosa dall'Autorità e prevede, per tutte le operazioni di trattamento, il rispetto di elevati *standard* di sicurezza. I dati sanitari contenuti nel Registro sono infatti trattati mediante codici identificativi, in modo tale da tutelare l'identità e la riservatezza dei malati. Sono previste, inoltre, rigorose misure per la custodia e la sicurezza dei dati, quali, in particolare, l'uso del certificato digitale (per identificare le postazioni di lavoro utilizzate per i trattamenti dei dati), l'utilizzo di canali di trasmissione protetti, la cifratura dei dati con chiave asimmetrica, la conservazione dei *log* delle operazioni effettuate e sistemi di "*strong authentication*". È vietato, infine, utilizzare dispositivi automatici che consentano di consultare i dati in forma massiva.

I dati raccolti nel Registro possono essere pubblicati a fini statistici solo in forma aggregata, in modo da rendere impossibile l'identificazione dei malati e possono essere condotti studi e ricerche solo nel rispetto di adeguate garanzie. Inoltre le informazioni possono essere comunicate ai registri tumori di altre regioni, ove questi siano legittimamente istituiti e

regolamentati, previe apposite convenzioni per garantire adeguati livelli di protezione dei dati. Il personale incaricato al trattamento deve infine rispettare regole di condotta analoghe al segreto professionale, anche quando non sia a ciò tenuto per legge.

Per ciò che concerne i trattamenti di dati a fini di ricerca scientifica, va anche menzionato il parere reso all'Istituto superiore di sanità (Iss) (provv. 17 gennaio 2013 [doc. web. n. 2298929]) su uno schema di regolamento che modifica il regolamento per i trattamenti di dati sensibili e giudiziari emanato dall'Iss il 17 luglio 2007 (v. parere favorevole del Garante provv. 28 febbraio 2007 [doc. web n. 1390743]), per finalità di trasparenza, razionalizzazione e semplificazione nella programmazione della ricerca. Le modifiche hanno riguardato soltanto la scheda che individua i tipi di dati sensibili che possono essere trattati e le operazioni eseguibili nelle attività di ricerca scientifica e statistica dell'Iss ai sensi dell'art. 98 del Codice.

Il nuovo regolamento tiene conto delle indicazioni ufficiose dell'Autorità che hanno riguardato, in particolare: le garanzie da assicurare sia nei trattamenti effettuati per scopi statistici e di ricerca scientifica nell'ambito del Sistema statistico nazionale (Sistan), sia nei trattamenti, svolti al di fuori del Sistan, per attività di ricerca scientifica in campo medico, biomedico ed epidemiologico; l'individuazione dell'ambito di comunicazione dei dati sensibili trattati e la previsione di opportune cautele a tutela della riservatezza degli interessati.

4.1.1. I regolamenti degli enti locali

Anche nel 2012 sono pervenute richieste di parere da parte degli enti locali relativamente a trattamenti di dati sensibili o giudiziari.

Come già evidenziato nelle precedenti Relazioni (cfr. da ultimo Relazione 2011, p. 52) l'Autorità ha espresso nel 2005 parere positivo sullo schema tipo di regolamento predisposto da Anci, Upi e Uncem [doc. web nn. 1174532 e 1170239], nonché sugli ulteriori trattamenti di dati sensibili e giudiziari non considerati nel suddetto schema tipo (parere 29 dicembre 2005 [doc. web n. 1213424]). Nel 2006 l'Autorità ha inoltre formulato un parere richiesto dall'Unione statistica dei comuni italiani (Usci) [doc. web nn. 1298732 e 1315375] riguardante i trattamenti di dati sensibili e giudiziari effettuati dagli uffici di statistica comunali per scopi di ricerca statistica nell'ambito del Sistan non ricompresi nel Psn.

In questo quadro l'Autorità ha comunicato agli enti locali richiedenti che occorre chiedere un nuovo parere al Garante solo nel caso in cui si intendano effettuare ulteriori trattamenti di dati sensibili e giudiziari ovvero operazioni non considerate nel predetto schema tipo predisposto dall'Anci o nei citati pareri del Garante (art. 20, comma 2, del Codice) (nota 6 luglio 2012).

4.2. LA TRASPARENZA DELL'ATTIVITÀ AMMINISTRATIVA E L'ACCESSO AI DOCUMENTI AMMINISTRATIVI

Le tematiche riguardanti l'accesso ai documenti amministrativi continuano ad essere oggetto di intervento del Garante a causa di molteplici segnalazioni e richieste di chiarimenti, da parte di pubbliche amministrazioni e cittadini.

Tra i casi più rilevanti si registra il quesito di un comune in ordine alla possibilità di rendere ostensibili, ad una testata giornalistica, i nominativi dei titolari dei *pass* per accedere alla zona a traffico limitato. In proposito l'Ufficio ha evidenziato che, nell'ipotesi in cui l'amministrazione ritenga di accogliere la richiesta di accesso nel rispetto dei princìpi di indispensabilità, pertinenza e non eccedenza (artt. 11, comma 1, lett. *d)*, e 22 del Codice), occorre adottare opportune cautele al fine di non rendere ostensibili dati eccedenti rispetto all'interesse ed ai motivi sottesi all'istanza medesima. Sono state pertanto valutate positivamente le misure individuate dal comune, che aveva dichiarato l'intenzione di omettere l'indicazione dei soggetti aventi diritto per ragioni di salute-disabilità, nonché la residenza e il domicilio. Tali indicazioni sono state sottoposte all'esame del Collegio che ne ha preso atto (nota 4 ottobre 2012).

Anche le problematiche riguardanti l'accesso di consiglieri comunali e provinciali agli atti dell'ente di riferimento sono state sottoposte all'attenzione del Garante, in particolare da una società partecipata, in un quesito relativo al diritto di accesso dei consiglieri. Sul punto è stato ricordato che la disciplina di riferimento demanda al soggetto interpellato -che non dovrà chiedere alcun consenso agli interessati (art. 24, comma 1, lett. *a)*, del Codice), né alcuna autorizzazione all'Autorità-, l'obbligo di accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* dei consiglieri degli enti locali interessati, nel rispetto dei limiti e delle condizioni di legge (art. 43, comma 2, d.lgs. n. 267/2000) (nota 1° ottobre 2012).

Per quanto riguarda il tema della trasparenza e della pubblicazione in internet di dati personali sono pervenute numerose istanze sul corretto trattamento dei dati contenuti negli atti e delibere pubblicati sui siti web di organi costituzionali, ministeri, regioni ed enti locali.

Per quanto riguarda gli organi costituzionali rimane aperto il problema della reperibilità in internet, anche attraverso i motori di ricerca generalisti, di dati personali -in alcuni casi, sensibili e giudiziari- contenuti in atti parlamentari pubblicati nei siti web di Camera e Senato.

Al riguardo il Garante ha evidenziato che i lavori delle istituzioni parlamentari sono soggetti a un regime di pubblicità puntualmente disciplinato (art. 65 del regolamento della Camera e art. 33 del regolamento del Senato) e che i princìpi inerenti al trattamento dei dati sensibili e giudiziari sono applicabili ai trattamenti svolti dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale *"in conformità ai rispettivi ordinamenti"* (art. 22, comma 12, del Codice). Attualmente la posizione della Camera è documentata nel resoconto della riunione dell'Ufficio di presidenza del 26 giugno 2008 in cui si afferma che alle richieste di cancellazione o di modifica degli atti parlamentari pubblicati sul sito della Camera *"allo stato, non può che darsi risposta negativa alla luce del regime costituzionale della pubblicità dei lavori parlamentari e della non modificabilità dei relativi atti"*.

In proposito questa Autorità -nel rispetto dell'autonomia costituzionale della Camera- ha evidenziato, come già in passato (cfr. Relazione del 2007 e discorso del Presidente 16 luglio 2008), l'opportunità di una attenta riflessione sul tema, in particolare quando la diffusione riguardi dati sensibili o comunque meritevoli di protezione (nota 22 dicembre 2012; note 9 e 10 gennaio 2013).

Per la generalità delle pubbliche amministrazioni, il Garante ha emanato il provvedimento del 2 marzo 2011 recante le "Linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" (in G.U. 19 marzo 2011, n. 64 [doc. web n. 1793203] cfr. Relazione 2011 p. 56).

In argomento è stato sollevato, tra gli altri, il problema della diffusione di dati personali contenuti in atti e deliberazioni pubblicati sull'albo pretorio *online* degli enti locali. In merito, l'Autorità ha ricordato in particolare che, in base alla disciplina di settore, tutte *"le deliberazioni del comune e della provincia sono pubblicate mediante affissione all'albo pretorio, nella sede dell'ente, per quindici giorni consecutivi, salvo specifiche disposizioni di legge*" (art. 124, comma 1, d.lgs. 18 agosto 2000 n. 267 recante il "Testo unico delle leggi sull'ordinamento degli enti locali"). Nel richiamato provvedimento del 2 marzo 2011 recante le linee-guida in materia, il Garante ha indicato che trascorsi "*i predetti periodi di tempo specificatamente individuati, determinate notizie, documenti o sezioni del sito devono essere rimossi dal web o privati degli elementi identificativi degli interessati*" (cfr. *infra* par. 5.2.). Fra i numerosi casi esaminati, si segnala il provvedimento con il quale il Garante ha dichiarato la illiceità del trattamento effettuato da un comune e ha vietato di diffondere in internet, oltre i quindici giorni previsti per la pubblicazione nell'albo pretorio, i dati personali di un cittadino contenuti in una deliberazione della giunta comunale (provv. 23 febbraio 2012 [doc. web n. 1876679]).

Numerose incertezze manifestate dalle pp.aa. hanno riguardato la pubblicazione dei dati di soggetti beneficiari di aiuti economici, per i quali l'Autorità ha richiamato i princìpi espressi nelle citate linee-guida, relativi alla pubblicazione degli elenchi di beneficiari di provvidenze economiche e di altri atti che riconoscono agevolazioni, sussidi o altri benefici. In tali elenchi possono essere riportati i soli dati necessari all'individuazione dei soggetti interessati (nominativi e relativa data di nascita), l'esercizio finanziario relativo alla concessione del beneficio, nonché l'indicazione della "…*disposizione di legge sulla base della quale hanno luogo le erogazioni*" medesime (art. 1, comma 2, d.P.R. n. 118/2000). Non risulta invece giustificato diffondere ulteriori dati quali l'indirizzo di abitazione, il codice fiscale, le coordinate bancarie relative all'accredito dei contributi, la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente (Isee) ovvero informazioni che descrivano le condizioni di indigenza in cui versa l'interessato. Non devono inoltre essere riportate negli albi diffusi *online* informazioni idonee a rivelare lo stato di salute degli interessati (artt. 22, comma 8 e 68, comma 3, del Codice).

L'Autorità, richiamando il Codice e le predette linee-guida, ha inoltre più volte dichiarato l'illiceità del trattamento effettuato da soggetti pubblici per aver diffuso sul web dati idonei a rivelare lo stato di salute in violazione delle norme citate.

Nello specifico, il Garante è intervenuto, fra l'altro, nei confronti di un comune, di una Asl e di una azienda regionale per il diritto allo studio universitario per vietare l'ulteriore diffusione in internet dei dati sulla salute di cittadini disabili e di persone che hanno beneficiato di rimborsi per spese sanitarie (provv. 22 novembre 2012 [doc. web n. 2194472]; provv. 29 novembre 2012 [doc. web n. 2192671]; provv. 19 dicembre 2012 [doc. web n. 2223692]. In tutti questi casi, con separato procedimento l'Autorità si è riservata di valutare gli estremi per contestare ai predetti soggetti pubblici la sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, del Codice.

Lo stesso divieto di diffusione di dati idonei a rivelare lo stato di salute è stato richiamato anche con riferimento agli obblighi di pubblicazione gravanti sulle pp.aa. alla luce dell'art. 18 (rubricato "amministrazione aperta") del d.l. 22 giugno 2012 n. 83, convertito dalla l. n. 134 del 7 agosto 2012, recante "Misure urgenti per la crescita del Paese" (cd. "decreto sviluppo"). In dettaglio, un'azienda sanitaria aveva chiesto se il predetto art. 18 la obbligasse a pubblicare su internet anche i dati dei pazienti che avevano ricevuto indennizzi per danni irreversibili causati da vaccinazioni o dalla somministrazione di emoderivati, o altri contributi legati a patologie mediche certificate. L'Autorità ha chiarito che, per quanto riguarda le persone fisiche, l'articolo citato prevede la pubblicazione *online* solo dei dati di chi riceve "*corrispettivi o compensi*" escludendo la diffusione delle informazioni menzionate, chiaramente idonee a rivelare lo stato di salute dei soggetti interessati (nota 12 ottobre 2012).

Infine, sempre in materia di trasparenza, si segnalano alcuni interventi per richiamare l'attenzione sulla necessità che la diffusione di dati personali sia sempre prevista da idonei presupposti normativi. Al riguardo, si ricorda il caso di un comune che ha pubblicato sul proprio sito istituzionale l'elenco dei destinatari dei verbali elevati per abbandono irregolare dei rifiuti; il Garante ha ritenuto tale condotta non conforme alla disciplina applicabile in materia, poiché i dati erano stati diffusi in assenza di idonei presupposti normativi (art. 19, comma 3, del Codice) (nota 2 novembre 2012).

4.2.1. Anagrafe nazionale degli abilitati alla guida

L'Autorità ha esaminato l'istanza di un cittadino che lamentava la mancata registrazione, presso l'Anagrafe nazionale degli abilitati alla guida, della totalità delle annotazioni intervenute nel tempo comportanti la variazione del punteggio della patente (decurtazioni e attribuzioni di punti).

Alla luce dell'istruttoria preliminare effettuata dall'Ufficio è risultato, in particolare, che l'organo da cui dipende l'agente che ha accertato la violazione comportante la perdita di punteggio, deve darne notizia, entro trenta giorni dalla definizione della contestazione, alla predetta Anagrafe (art. 226, commi 10, 11, 12 e art. 126-*bis*, comma 2, d.lgs. 30 aprile 1992, n. 285); ed inoltre ogni variazione di punteggio deve essere comunicata agli interessati da parte dell'Anagrafe stessa e ciascun conducente può controllare in tempo reale lo stato della propria patente (art. 126-*bis*, comma 3, del nuovo codice della strada).

In termini generali, peraltro, le informazioni personali -anche quelle contenute in banche dati pubbliche- devono essere trattate secondo correttezza, esatte e, se necessario, aggiornate (art. 11, comma 1, lett. *a)*, *c)*, *d)*, del Codice).

Dalla documentazione prodotta è emerso, invece, che la comunicazione effettuata dal Ministero delle infrastrutture e dei trasporti non conteneva talune variazioni di punteggio e che le stesse non erano annotate neppure nell'estratto conto dei punti, reso disponibile al reclamante consultando il portale di servizi di *e-government* del Dipartimento trasporti del Ministero delle infrastrutture e dei trasporti (www.ilportaledellautomobilista.it); pertanto, entrambe le modalità con cui l'amministrazione rende note all'interessato le variazioni di punteggio sono costituite da estratti cronologici che non contengono, nel dettaglio e cronologicamente, la totalità delle stesse variazioni, anche se effettuate attraverso procedure automatiche. In sintesi, è stato, quindi, rilevato che i dati contenuti negli estratti cronologici non sono esatti e completi.

Il Garante ha pertanto prescritto al predetto Ministero che le future comunicazioni agli interessati (anche nel caso di consultazione diretta da parte dell'interessato attraverso il cd. "portale dell'automobilista") debbano contenere i dati relativi alla totalità delle variazioni dei punti della patente, comprese quelle effettuate in modo automatizzato, di attribuzione di punti (*bonus*) e successiva decurtazione per illegittima attribuzione.

Per quanto riguarda gli eventi passati, il Garante ha prescritto, altresì, che qualora l'interessato ne faccia specifica richiesta, sia assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazione di punteggio della patente (provv. 24 gennaio 2013 [doc. web n. 2256617]).

4.3. LA DOCUMENTAZIONE ANAGRAFICA E LE LISTE ELETTORALI

Nel periodo di riferimento, si segnala, tra gli altri, il caso di una cittadina britannica, coniugata con un cittadino italiano, che aveva lamentato l'inesattezza di alcuni dati contenuti nell'estratto dell'atto di matrimonio. In merito è stato fatto presente che il Codice sancisce per l'interessato il diritto di accedere ai propri dati personali e fra l'altro, di ottenere "*l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati*" (art. 7, comma 3, lett. *a)*), mediante richiesta rivolta al titolare o al responsabile del trattamento dei dati personali (art. 8, comma 1, e artt. 145 e 146 del Codice) (nota 18 ottobre 2012).

In un diverso caso, un cittadino si era rivolto all'Autorità chiedendo se, ai fini dell'iscrizione nell'Anagrafe della popolazione residente e della sottoscrizione del contratto per la fornitura dell'acqua potabile di un suo inquilino, fosse legittima la richiesta avanzata dal comune di ottenere fotocopia integrale del contratto di locazione. In proposito è stato osservato che in base alla disciplina di settore l'ufficiale di anagrafe, al fine di verificare la sussistenza del requisito della dimora abituale di chi richiede l'iscrizione anagrafica, è tenuto ad effettuare gli accertamenti necessari ad appurare la verità dei fatti denunciati dagli interessati, potendo invitare gli stessi a fornire le notizie e i chiarimenti necessari alla regolare tenuta dell'Anagrafe (art. 4 l. 24 dicembre 1954, n. 1228 e art. 19 d.P.R. 30 maggio 1989, n. 223) (nota 23 agosto 2012).

Il Ministero dell'interno ha chiesto all'Autorità se, per i profili di competenza in materia di protezione dei dati personali, un consiglio notarile potesse accedere, in via telematica, "*all'archivio informatico dei cartellini delle carte di identità*" detenuto da un comune, al fine di effettuare le verifiche necessarie a contrastare furti di identità, principalmente in danno di istituti di credito. Sul punto è stato sottolineato che i comuni possono comunicare dati anagrafici anche con strumenti automatizzati e per via telematica, per finalità di snellimento

ed efficienza dell'azione amministrativa a supporto del cittadino, nel rispetto, tuttavia, degli specifici divieti di consultazione diretta degli atti anagrafici stabiliti dall'art. 37 d.P.R. n. 223/1989 (nota 29 agosto 2012). Spetta, pertanto, al comune interpellato verificare che l'accesso ai cartellini della carta di identità di cui all'art. 290 r.d. 6 maggio 1940, n. 635, avvenga in conformità ai presupposti stabiliti dalla disciplina di settore e nel rispetto delle misure di sicurezza stabilite dal Codice. Quanto all'esigenza di contrastare i furti di identità, sono state richiamate le specifiche disposizioni che prevedono in particolare che siano assoggettati a riscontro "*documenti di identità e di riconoscimento, comunque denominati o equipollenti, ancorché smarriti o rubati*" (artt. 30-*ter* e 30-*quinquies*, comma 1, lett. *a)*, d.lgs. 13 agosto 2010 n. 141, modificato dal d.lgs. 11 aprile 2011, n. 64).

Una delicata questione sottoposta all'Autorità ha riguardato la richiesta, presentata dai comuni alle strutture sanitarie presso le quali si sono verificati i parti, di riportare negli attestati di avvenuta nascita -all'atto della dichiarazione di nascita- le generalità delle puerpere che non hanno voluto riconoscere il proprio figlio (nota 25 luglio 2012). In base al quadro normativo di settore, nell'atto di nascita vanno indicate, tra le altre informazioni, le generalità dei genitori solo nei casi in cui questi ultimi "*hanno espresso con atto pubblico il proprio consenso ad essere nominati*" (artt. 29, comma 2, e 30, commi 1 e 2, d.P.R. 3 novembre 2000, n. 396) nel rispetto delle specifiche cautele previste dalle norme vigenti a tutela dell'anonimato della madre che abbia eventualmente scelto alla nascita di non voler essere nominata (v. ad es., per quanto riguarda le informazioni da riportare sul certificato di assistenza al parto, l'art. 93, comma 1, del Codice; l'art. 30, comma 1, d.P.R. n. 396/2000 e l'allegato- parte II d.m. 16 luglio 2001, n. 349). Sul punto è stata fornita ai comuni la posizione del Ministero dell'interno - Direzione centrale per i servizi demografici, il quale si è espresso nel senso di ritenere che "*L'attestazione di nascita deve contenere i dati della puerpera anche quando la medesima non intende effettuare il riconoscimento, perché il riconoscimento deve essere fatto al momento della formazione dell'atto di nascita e non può essere rimesso al momento della redazione dell'attestazione di nascita da parte dell'ostetrica o di chi ha assistito al parto. La mancanza delle generalità della puerpera, oltre a costituire un falso, si presterebbe anche ad uso illecito: se la donna non vuole riconoscere il figlio, ma il riconoscimento vuole essere fatto dall'uomo che si dichiara il*

padre, un eventuale attestazione di nascita senza il nome della puerpera consentirebbe all'uomo di presentarsi a rendere la dichiarazione di nascita, favorendo il riconoscimento da parte di altra donna che si dichiarasse madre congiuntamente all'uomo".

In relazione al rilascio delle attestazioni di stato civile, l'Autorità è intervenuta sul caso di un uomo che contestava ad un comune di aver rilasciato a un avvocato, che agiva privo di delega per conto di alcuni parenti dell'interessato, la copia integrale del suo atto di nascita, recante le informazioni sul provvedimento giudiziario riguardante la sua adozione.

L'Autorità, interpellata dal difensore civico al quale l'interessato aveva chiesto aiuto, ha però evidenziato che in base alla normativa vigente qualunque attestazione di stato civile riferita all'adottato può essere rilasciata solo con l'indicazione del nuovo cognome e con l'esclusione di qualsiasi riferimento alla paternità e alla maternità del minore (artt. 26, comma 4, e 28, comma 2, l. 4 maggio 1983, n. 184; artt. 106 e 107, commi 1 e 2, lett. *b)*, d.P.R. 3 novembre 2000, n. 396; art. 177, comma 3, del Codice), poiché indicazioni sul rapporto di adozione possano essere fornite solo su espressa autorizzazione dell'autorità giudiziaria.

Il Garante ha quindi vietato ai parenti dell'interessato l'ulteriore utilizzo delle informazioni sull'adozione contenute nella copia dell'atto di nascita. Ha poi prescritto al comune di fornire al proprio personale di stato civile adeguate istruzioni per evitare ulteriori violazioni sui dati relativi alle persone adottate. Il provvedimento è stato inoltre trasmesso all'autorità giudiziaria che potrà valutare gli eventuali illeciti penali commessi (provv. 8 novembre 2012 [doc. web n. 2187244]).

Si evidenzia ancora che un comune aveva chiesto chiarimenti in ordine alla richiesta di rilascio di copia delle liste elettorali, formulata da una società per effettuare un'indagine "*sulla rilevazione indici di ascolto e di diffusione mezzi di comunicazione*". Al riguardo, è stato evidenziato preliminarmente che il Garante si è espresso sull'argomento in varie occasioni (v. Relazione 2005 p. 65; Relazione 2006 p. 46; Relazione 2008 p. 63) specificando che le liste elettorali possono essere duplicate solo "*per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso*", secondo quanto disposto dall'art. 177, comma 5, del Codice. Spetta all'amministrazione destinataria dell'istanza di

ostensione valutare se la finalità dichiarata dal richiedente sia conforme all'attività svolta dal soggetto medesimo e se rientri effettivamente tra le ipotesi di cui al citato art. 177 del Codice. I dati personali estratti dalle liste elettorali eventualmente acquisite indebitamente non potranno essere utilizzati (art. 11, comma 2, del Codice), ferme restando le sanzioni di legge, l'adozione di ogni eventuale provvedimento inibitorio e le eventuali denunce all'autorità giudiziaria delle violazioni riscontrate (nota 25 settembre 2012).

Un ulteriore caso ha riguardato la richiesta presentata da Ancitel S.p.A. di ottenere copia delle liste elettorali in qualità di responsabile del trattamento designata da taluni enti *non profit*, che agiscono quali titolari del trattamento per finalità comprese tra quelle previste dalle vigenti disposizioni in materia (art. 51, comma 5, d.P.R. n. 223/1967, come modificato dall'art. 177, comma 5, del Codice). Nella richiesta era previsto che i predetti dati sarebbero stati successivamente trasmessi per l'elaborazione a Consodata S.p.A. anch'essa designata responsabile e da questa consegnati ai suddetti enti.

A tal proposito è stato rappresentato dall'Ufficio che le organizzazioni non lucrative, legittimate ad ottenere dai comuni il rilascio di copia delle liste elettorali e ad utilizzarle per il perseguimento delle finalità individuate dalla normativa vigente, possono richiedere a soggetti esterni (nel caso di specie Ancitel S.p.A. e Consodata S.p.A.) lo svolgimento di specifiche operazioni di trattamento. I dati, però, non possono essere comunicati ad altri titolari e possono essere utilizzati solo per le finalità perseguite dagli enti titolari del trattamento riconducibili a quelle tassativamente individuate dal citato art. 51, comma 5, del d.P.R. n. 223/1967 (nota 29 agosto 2012).

4.4. L'ISTRUZIONE

4.4.1. La scuola

Nel corso degli anni 2011 e 2012 l'Autorità ha in più occasioni fornito chiarimenti in relazione al trattamento di dati personali correlato all'istruzione pubblica.

In particolare, era stato segnalato che la ditta incaricata da una scuola pubblica di gestire il servizio di refezione scolastica inviava alle famiglie i "bollettini" non in busta chiusa, e con l'indicazione della quota spettante ad ogni bambino, consentendo così anche a soggetti non

legittimati di venire a conoscenza delle informazioni idonee a rivelare la situazione economica degli interessati. A seguito dell'intervento dell'Autorità, la predetta scuola ha garantito che i "bollettini" sarebbero stati inviati in busta chiusa sigillata (nota 7 dicembre 2011).

Con un'altra segnalazione veniva rappresentato che una scuola aveva pubblicato sul proprio sito istituzionale una circolare del dirigente scolastico indirizzata al personale docente, contenente l'indicazione dei nominativi degli alunni con specifici disturbi di apprendimento insieme ad altre informazioni relative alle loro condizioni di salute. Nell'ambito dell'istruttoria, il titolare del trattamento, nel confermare l'accaduto, ha fornito idonee assicurazioni concernenti, in particolare, l'avvenuta rimozione del documento dal web, nonché dalle copie *cache* dei principali motori di ricerca. Su tale base l'Ufficio, pur avendo riscontrato una condotta non conforme alla disciplina applicabile, non ha ritenuto sussistenti i presupposti per l'adozione di un provvedimento prescrittivo o inibitorio dell'Autorità, salva la valutazione dei presupposti per contestare la violazione del divieto di diffondere dati sensibili (art. 162, comma 2-*bis,* del Codice) (nota 9 novembre 2011).

Analogamente un istituto scolastico pubblico ha chiesto all'Autorità se l'informazione relativa alla presenza di disturbi specifici di apprendimento debba considerarsi un dato sensibile, ai sensi dell'art. 4, comma 1, lett. *d)*, del Codice.

Al riguardo, l'Ufficio ha evidenziato che i disturbi specifici di apprendimento sono considerati, dalle ricerche più accreditate, disturbi di origine neurobiologica e, in base alla normativa di settore, devono essere diagnosticati dal Servizio sanitario nazionale, sicché le relative informazioni costituiscono dati sensibili in quanto idonei a rivelare lo stato di salute degli interessati, ai sensi del Codice (art. 3, l. 8 ottobre 2010, n. 170; "Linee-guida per il diritto allo studio degli alunni e degli studenti con disturbi specifici di apprendimento" allegate al decreto del Ministro dell'istruzione dell'università e della ricerca n. 5669, del 12 luglio 2011; art. 4, comma 1, lett. *d)*, del Codice).

Tali dati devono quindi essere trattati nel rispetto delle più stringenti regole poste dal Codice per tale categorie di informazioni e della specifica normativa di settore sopra richiamata (cfr. artt. 13, 20 e 22 del Codice; regolamento adottato dal Ministero della pubblica istruzione per i trattamenti dei dati sensibili e giudiziari da effettuarsi presso il

medesimo Ministero, le istituzioni scolastiche ed educative e gli istituti regionali di ricerca educativa -si veda in particolare la scheda n. 4- d.m. 7 dicembre 2006, n. 305, sul quale il Garante ha espresso il parere di competenza in data 26 luglio 2006 [doc. web n. 1321703]) (nota 23 gennaio 2013).

La *privacy* a scuola. *Vademecum*

Prima dell'apertura dell'anno scolastico 2012-2013, l'Autorità ha pubblicato un *pamphlet,* intitolato "La *privacy* a scuola", quale contributo a favore di professori, genitori e studenti, recante alcune indicazioni generali in materia di protezione dei dati personali (6 settembre 2012 [doc. web n. 1923387]).

In tale ambito, il Garante ha precisato che possono essere assegnati temi riguardanti profili o esperienze personali affidando, qualora gli elaborati vengano letti in classe, alla sensibilità degli insegnanti la ponderazione tra esperienze didattiche e tutela della riservatezza.

Con riferimento all'uso di cellullari e *tablet* a scuola l'Autorità, nel ribadire che spetta agli istituti scolastici decidere come regolamentare l'uso di tali strumenti, ha precisato che essi possono essere utilizzati esclusivamente per fini strettamente personali (come per la ripresa e gli scatti fotografici di recite, saggi e gite scolastiche) e che non possono essere diffuse immagini, video o foto sul web se non con il consenso degli interessati.

Non possono, inoltre, essere diffusi sul sito *internet* della scuola i dati personali relativi agli studenti beneficiari di agevolazioni per il servizio di refezione scolastica ovvero dei genitori in ritardo con il pagamento della retta o del servizio di mensa. Salvi avvisi di carattere generale, le scuole devono, infatti, effettuare comunicazioni di carattere individuale per rivolgersi a singoli e specifiche persone.

Le telecamere installate all'interno delle scuole possono funzionare solo negli orari di chiusura degli istituti ed è sempre, comunque, necessario fornire un'idonea informativa sul trattamento dei dati personali effettuato tramite tali strumenti (art. 13 del Codice). Le telecamere installate all'esterno delle scuole possono, invece, riprendere solo aree strettamente pertinenti l'edificio (v. *infra* par. 4.6.).

La raccolta di informazioni personali per attività di ricerca attraverso questionari da sottoporre agli studenti è consentita solo su base volontaria, se ragazzi e genitori sono stati prima informati sugli scopi della ricerca, le modalità di trattamento e le misure di sicurezza adottate.

L'Autorità ha ribadito, inoltre, che su esplicita richiesta degli interessati e previa idonea informativa (art. 13 del Codice), le scuole e gli istituti scolastici di istruzione secondaria, per agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità. Tali dati possono essere successivamente trattati esclusivamente a tali fini (art. 96 del Codice).

Nel ricordare il regime di pubblicità dei voti dei compiti in classe e delle interrogazioni, degli esiti degli scrutini o degli esami di Stato, i cui profili di trasparenza e conoscibilità sono comunque stabiliti dal Ministero dell'istruzione, il Garante ha precisato che è necessario che non vengano divulgate, anche indirettamente, informazioni sulle condizioni di salute degli studenti, quali il riferimento alle "prove differenziate" sostenute dai portatori di *handicap*.

L'Autorità ha anche ribadito l'obbligo per le scuole di fornire agli interessati un'idonea informativa sul trattamento dei loro dati personali e di prestare particolare attenzione alle più stringenti regole poste dal codice per il trattamento dei dati sensibili e giudiziari (artt. 20-22, 26 e 27 del Codice), ricordando a studenti e genitori i loro diritti di accesso alle informazioni che li riguardano, di rettifica e aggiornamento delle stesse (art. 7 del Codice).

L'Autorità ha, infine, auspicato che vengano previste adeguate misure di sicurezza a protezione dei dati nei provvedimenti del Ministero dell'istruzione relativi, in particolare, all'iscrizione *online* degli studenti, all'adozione dei registri *online* e alla consultazione della pagella via web, sui quali il Garante deve esprimere il proprio parere ai sensi dell'art. 154 comma 4, del Codice.

Anagrafe degli studenti

Il Garante ha formulato parere contrario, per le ragioni di seguito sintetizzate, sullo schema di Accordo tra il Ministero dell'istruzione, dell'università e della ricerca (Miur), il Ministero del lavoro e delle politiche sociali, le regioni, le Provincie autonome di Trento e Bolzano, Anci, Upi, volto a garantire l'integrazione e l'interoperabilità dell'Anagrafe nazionale degli studenti (Ans) con le Anagrafi regionali degli studenti (Ars), nell'ambito del Sistema nazionale delle anagrafi (art. 3, comma 4, d.lgs. 15 aprile 2005, n. 76).

Al riguardo l'Autorità ha individuato numerosi profili di criticità riguardanti sia i

presupposti di legittimità del trattamento dei dati personali degli studenti, sia le modalità del trattamento e la sicurezza dei dati stessi ed ha segnalato il rischio di duplicazione delle informazioni delle banche dati.

Il Garante ha in particolare evidenziato che, in via generale, sono "interoperabili" quei sistemi idonei a garantire l'intellegibilità dei dati da parte di soggetti diversi, nonché l'univocità interpretativa e la "leggibilità" del dato anche al di fuori del suo contesto iniziale.

L'Autorità ha, poi, precisato che il divieto di duplicazione di banche dati si fonda sui princìpi costitutivi della normativa in materia di protezione dei dati personali. Infatti, affinché i dati siano esatti e aggiornati è necessario, in primo luogo, prevedere l'alimentazione di un'unica banca dati, consultabile dai soggetti legittimati (art. 11 del Codice).

Ha evidenziato, inoltre, che il sistema di accessi da parte delle regioni e degli enti locali alle anagrafi del sistema non è risultato conforme alla normativa, in base alla quale le regioni e gli enti locali possono accedere all'Ans in relazione alle proprie competenze istituzionali (d.l. n. 179/2012, convertito in l. n. 221/2012). Al riguardo, il Garante ha precisato che a tal fine possono essere trattate informazioni pertinenti e non eccedenti rispetto ad una specifica funzione. I dati personali e le specifiche funzioni istituzionali per le quali tali dati sono ritenuti necessari devono, pertanto, essere preventivamente individuati in uno o più atti amministrativi attuativi della predetta norma da sottoporre al parere del Garante (artt. 11, 18, comma 2, 19, comma 1, 154, comma 1, lett. *g),* e comma 4 del Codice).

In tale quadro, l'Autorità ha inoltre rilevato che le generiche funzioni di programmazione possono essere realizzate tramite informazioni aggregate che non consentono di identificare l'interessato.

L'Autorità ha altresì rilevato, come specifica criticità inerente aspetti di legittimità, che lo schema di accordo prevedeva l'accesso da parte dell'ufficio di statistica del Ministero del lavoro e delle politiche sociali ai dati personali contenuti nell'Ans, senza adeguata previsione in tal senso della normativa di settore.

È stata inoltre evidenziata, con specifico riferimento al "gestore del sistema informativo regionale" inteso come "amministratore di sistema", la mancata conformità a quanto previsto nel provvedimento del Garante 27 novembre 2008 [doc. web n. 1577499], in quanto

all'amministratore veniva consentito di conoscere pienamente i dati contenuti nel sistema mentre, in base al citato provvedimento, le sue mansioni sono "*finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti*" senza che vi sia "*una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni)*".

Specifiche criticità sono state individuate, infine, in riferimento al sistema di codifica dei dati che avrebbe dovuto servire a garantire l'anonimato degli interessati. Il Garante ha, infatti, rilevato che la procedura di codifica, prevedendo unicamente l'attribuzione di un codice meccanografico ad ogni singolo studente, ricollegato ai dati personali dello stesso, ancorché presenti in un'altra tabella, senza specificare in particolare il criterio di accesso alla tabella di decodifica, non appariva idonea a garantire l'anonimizzazione dei dati né ad escludere che gli interessati potessero essere identificabili (parere 24 gennaio 2013 [doc. web n. 2304850]).

Diffusione sul sito web di dati personali relativi agli studenti

Nel corso dell'anno di riferimento, è stato altresì segnalato che una scuola pubblica superiore diffondeva sul proprio sito internet istituzionale l'elenco degli studenti distinti per classe. Tale diffusione, che sarebbe stata effettuata per finalità di trasparenza e pubblicità amministrativa non risultava, tuttavia, prevista da alcuna norma di legge o di regolamento (art. 19, comma 3, del Codice) (cfr. anche provv. 2 marzo 2011 [doc. web n. 1793203]).

Il Garante ha, pertanto, vietato alla scuola di diffondere ulteriormente i predetti dati personali sul proprio sito internet, salva la valutazione della sussistenza dei presupposti per contestare la violazione del divieto di diffondere dati personali in assenza di una norma di legge o di regolamento (art. 162, comma 2-*bis*, del Codice) (provv. 6 dicembre 2012 [doc. web n. 2217211]).

È stato, inoltre, segnalato che un istituto tecnico commerciale, nel diffondere sul proprio sito internet istituzionale le graduatorie relative alle supplenze del personale docente, aveva altresì consentito l'indicizzazione dei nomi degli interessati nei motori di ricerca esterni. Al riguardo, è stato evidenziato che i dati personali non devono essere liberamente reperibili utilizzando motori di ricerca esterni (cfr. art. 19, comma 3, del Codice; punto B delle citate linee-guida).

Il titolare del trattamento ha garantito di essersi conformato a tali indicazioni (nota 8 novembre 2012).

A seguito di una segnalazione, l'Ufficio ha potuto verificare che un istituto professionale aveva diffuso, sul proprio sito internet, una circolare recante l'indicazione dei nominativi degli alunni con disabilità e degli insegnanti di sostegno loro assegnati. A seguito dell'intervento dell'Ufficio l'istituto ha fornito idonee assicurazioni circa la rimozione dei predetti dati dalla rete internet.

L'Ufficio ha, tuttavia, disposto gli opportuni accertamenti per l'eventuale contestazione, con autonomo procedimento, della sanzione amministrativa di cui all'art. 162, comma 2-*bis*, del Codice per l'avvenuta violazione del divieto di diffusione dei dati sulla salute (nota 28 novembre 2012).

Flussi dati in ambito scolastico

L'Autorità è intervenuta a seguito di una comunicazione, ai sensi dell'art. 39, comma 1, lett. *a)*, del Codice, da parte di un istituto scolastico al quale un istituto superiore aveva chiesto di trasmettere dati relativi agli studenti del terzo anno della scuola secondaria di primo grado (nome, cognome indirizzo di residenza), per fornire agli stessi indicazioni relative alle nuove attività scolastiche proposte dall'istituto stesso.

Al riguardo, l'Ufficio ha ricordato, con riferimento all'attività di orientamento, che i soggetti pubblici, ivi comprese le scuole e gli istituti scolastici di istruzione secondaria possono, esclusivamente su richiesta degli interessati, comunicare e diffondere, anche per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità (art. 96 del Codice). Ha, comunque, rappresentato che un'adeguata iniziativa di orientamento può essere svolta dai singoli istituti mettendo, ad esempio, a disposizione degli studenti presso i diversi istituti scolastici, il materiale informativo che illustri le linee distintive dei vari percorsi formativi (nota 22 gennaio 2012).

4.4.2. L'università

Nel corso dell'anno, uno studente laureato ha formulato una richiesta di chiarimenti all'Autorità sulla possibilità di ottenere, a seguito dell'avvenuta rettificazione di attribuzione

di sesso, un nuovo diploma di laurea con indicati solo i nuovi dati anagrafici. Contestualmente, l'università competente ha rappresentato al Garante la propria intenzione di rilasciare all'interessato tale secondo diploma, opportunamente evitando di dar conto del fatto che la ristampa del diploma stesso era basata su una sentenza del tribunale, di rettificazione di attribuzione di sesso, passata in giudicato.

Tale soluzione è apparsa al Garante idonea a tutelare adeguatamente la dignità degli interessati e il diritto degli stessi a vedere correttamente rappresentata la propria identità sessuale a seguito della sua modificazione. Nel medesimo provvedimento il Garante ha, altresì, prescritto a tutte le università l'adozione, nell'ambito della propria autonomia, di idonei accorgimenti e cautele affinché non siano riportate nella relativa documentazione elementi idonei a rivelare l'avvenuta rettificazione di attribuzione di sesso. Ciò fermo restando il rispetto degli obblighi di conservazione dell'atto o del documento che contiene i dati personali dell'interessato ivi compreso il sesso e il nome originario. L'Autorità ha, infine, trasmesso il predetto provvedimento al Ministero dell'istruzione, dell'università e della ricerca ed alla CRUI (Conferenza dei Rettori delle Università Italiane) per la valutazione di eventuali iniziative volte ad orientare in modo corretto e omogeneo le procedure delle università in casi analoghi (provv. 15 novembre 2012 [doc. web n. 2121695]).

Un ricercatore universitario ha rappresentato all'Autorità che un ateneo, nel pubblicare sul proprio sito gli esiti relativi alle procedure per l'assegnazione di un posto da ricercatore, aveva reso tali documenti reperibili anche in internet attraverso i più comuni motori di ricerca. Al riguardo, l'Ufficio ha ribadito che i soggetti pubblici posso diffondere dati personali, diversi da quelli sensibili e giudiziari, se ammesso da una norma di legge o di regolamento ma quando tale diffusione avviene tramite la rete internet occorre individuare specifiche garanzie atte ad impedire l'indiscriminata ed incondizionata reperibilità delle informazioni (art. 19, comma 3, del Codice; provvedimento generale del 14 giugno 2007, recante "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" [doc. web n. 1417809]). Il titolare del trattamento ha conseguentemente fornito idonea assicurazione circa le misure assunte in conformità alle predette indicazioni del Garante (nota 12 luglio 2012).

Uno studente universitario ha segnalato all'Autorità che un ateneo aveva omesso di fornire l'informativa agli interessati e di indicare le finalità e modalità del trattamento, nonché i diritti di cui all'art. 7 del Codice (art. 13 del Codice). L'Ufficio ha quindi predisposto gli atti per l'applicazione della sanzione amministrativa (art. 161 del Codice). Con riferimento, inoltre, all'erogazione di servizi facoltativi che l'università intendeva rendere ai candidati al corso che lo studente intendeva frequentare (quali la comunicazione personale di informazioni di vario tipo, la promozione di iniziative culturali dell'università stessa o di terzi, nonché lo svolgimento di ricerche di mercato o di rilevazione del grado di soddisfazione sulla qualità dei servizi resi e sull'attività svolta dall'università), l'Ufficio ha precisato che l'ateneo è tenuto a rispettare la volontà degli interessati di beneficiarne o meno, acquisendo, di volta in volta, il loro specifico consenso al trattamento dei dati personali all'uopo necessari (nota 8 novembre 2012).

Trattamento di dati sensibili e giudiziari

La Provincia autonoma di Trento ha chiesto un parere al Garante sull'integrazione e aggiornamento del regolamento provinciale per il trattamento dei dati sensibili e giudiziari in relazione ai tipi di dati e alle operazioni eseguibili per le finalità di istruzione, educazione e formazione in ambito prescolare e scolastico e le relative finalità socio assistenziali, in ragione delle specifiche competenze attribuite dal legislatore alla Provincia stessa in materia di istruzione e formazione (artt. 68, 73, commi 1, lett. *a)* e *c)* e 2, lett. *a)* e *b)*, 86, comma 1, lett. *c)* e 95 del Codice).

In particolare, la Provincia, oltre ad aggiornare la vecchia scheda relativa all'istruzione, anche sulla base di indicazioni fornite dal Garante, ha inserito nel regolamento una nuova sezione sulle "*attività propedeutiche all'avvio dell'anno scolastico e attività educativa, didattica, formativa e di valutazione da parte delle istituzioni scolastiche e formative provinciali*", al fine di realizzare una più funzionale autonomia operativa, completando a livello provinciale, anche per il settore dell'istruzione, la disciplina del trattamento dei dati sensibili e giudiziari (parere 29 marzo 2012 [doc. web n. 1892028]).

4.5. ATTIVITÀ FISCALE E TRIBUTARIA

Sicurezza Anagrafe tributaria

Il Garante, con provvedimento del 18 settembre 2008 [doc. web n. 1549548], ha prescritto all'Agenzia delle entrate una serie di misure e accorgimenti in relazione ai livelli di

sicurezza degli accessi all'Anagrafe tributaria da parte dei soggetti esterni all'amministrazione finanziaria, prevedendo, in particolare, che l'Agenzia autorizzi i predetti accessi solo in seguito alla stipula di apposite convenzioni e che, annualmente, verifichi l'attualità delle finalità per cui ha concesso l'accesso anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni.

Su richiesta dell'Agenzia e dell'Anci, vista la rilevanza delle finalità istituzionali perseguite con i collegamenti all'Anagrafe tributaria da parte degli enti esterni, con il provvedimento del 16 febbraio 2011 [doc. web n. 1793806], il Garante ha prorogato il termine per tale adempimento al 15 aprile 2011, in considerazione della complessità delle attività da intraprendere, anche a fronte dell'incompleta diffusione della firma digitale presso tutti i comuni e delle difficoltà tecniche determinate dal forte afflusso di richieste pervenute sul sito dell'Agenzia per la sottoscrizione in modalità telematica della nuova convenzione.

Comunicazione integrativa annuale all'archivio dei rapporti finanziari presso l'Anagrafe tributaria

L'Agenzia delle entrate ha sottoposto al Garante lo schema di provvedimento, attuativo della recente normativa che ha introdotto nuove misure di contrasto all'evasione fiscale, riguardante le modalità con le quali le banche dovranno comunicare all'Anagrafe tributaria, per fini di controllo fiscale, le informazioni relative ai rapporti finanziari (ad es., per i conti correnti bancari, saldo iniziale e finale, importi totali degli accrediti e degli addebiti delle numerose tipologie di operazioni effettuate) (parere 17 aprile 2012 [doc. web n. 1886775]).

Tali dati, una volta raccolti, dovranno poi essere ordinati su scala nazionale per la formazione di specifiche liste di contribuenti a maggior rischio di evasione, secondo i criteri successivamente individuati con provvedimento del Direttore dell'Agenzia.

Anzitutto l'Autorità ha evidenziato che la normativa di cui lo schema è attuativo pone rilevanti problematiche relative alla protezione dei dati personali sia per l'eccezionale concentrazione presso l'Anagrafe tributaria di informazioni personali, sia in relazione alle finalità di classificazione degli interessati. Come più volte ribadito dall'Autorità -anche in sede di audizione presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria- non è, infatti, in discussione l'esigenza di disporre delle informazioni necessarie per l'azione di contrasto all'evasione fiscale, bensì l'integrale acquisizione e duplicazione presso l'Anagrafe

tributaria di una moltitudine di dati che, peraltro, genera un incremento esponenziale dei rischi e richiede misure di sicurezza di natura tecnica ed organizzativa particolarmente rigorose, sia per la trasmissione dei dati sia per la loro conservazione.

In questo quadro, in sede di istruttoria sono emerse numerose criticità relative in parte ad Entratel, il servizio telematico prescelto per la trasmissione dei dati (applicativo già in uso, oltre che per numerose comunicazioni di dati all'Anagrafe tributaria, anche per l'alimentazione dell'archivio dei rapporti finanziari), e in parte conseguenti agli aspetti tecnico-organizzativi dell'intera filiera di trattamento.

L'Agenzia ha richiesto, infatti, l'invio all'Anagrafe tributaria di una mole di dati che la gran parte degli operatori finanziari solitamente tratta con diversi sistemi applicativi, comportando quindi già all'origine una concentrazione di informazioni e, di conseguenza, un potenziale di rischio che difficilmente si riscontra nell'ordinario esercizio dell'attività benché le informazioni di base siano tutte nella disponibilità dell'operatore; infatti, solo questa specifica esigenza di conformità all'adempimento previsto dall'Agenzia rende necessaria l'aggregazione presso l'operatore medesimo, in un unico "oggetto informatico", della variegata tipologia di dati che risiederebbero altrimenti nelle diverse componenti applicative del sistema informativo.

Il Garante ha evidenziato che la scelta di utilizzare Entratel, se da un lato può semplificare l'assolvimento degli adempimenti perché già utilizzato per altre comunicazioni anche dagli operatori finanziari, dall'altro non consente di modulare le cautele rispetto alla specifica tipologia di dati che formano oggetto di ciascuna categoria di comunicazione. Entratel è risultato, infatti, inadeguato per soggetti di medio-grandi dimensioni in ragione delle voluminose quantità di scambio previste, rispetto alle potenzialità e alle limitanti caratteristiche tecniche dello strumento. Inoltre, pur rispettando le misure minime di cui all'Allegato B. al Codice, Entratel ha presentato ulteriori criticità che rendono necessario incrementarne i livelli di sicurezza per i soggetti di piccole dimensioni.

Da qui la prescrizione di dettagliate misure di sicurezza di seguito sintetizzate, da inserire nello schema di provvedimento, riguardanti sia il canale di comunicazione prescelto dall'Agenzia, sia le operazioni di trattamento dei dati finalizzate alla comunicazione delle

informazioni all'Anagrafe tributaria da parte degli operatori finanziari, volte ad assicurare, in particolare, che il procedimento di cifratura del *file* da trasmettere da parte dell'operatore finanziario possa avvenire già contestualmente alla estrazione dei dati dai sistemi, o, quantomeno, nella fase immediatamente successiva, preferibilmente con l'utilizzo di strumenti automatici.

L'Agenzia è stata pertanto invitata a predisporre l'uso di canali di comunicazione diversi e alternativi al servizio Entratel, soprattutto per le comunicazioni da parte di soggetti detentori di una elevata quantità di dati come i gruppi bancari, privilegiando l'interconnessione *application-to-application* tra i rispettivi sistemi informativi. Ciò consentirebbe di automatizzare il più possibile il processo di raccolta dei dati, rafforzando l'intera filiera di trattamento delle informazioni che, altrimenti, risulterebbero accessibili a una molteplicità di soggetti incaricati amplificando le possibilità di loro utilizzo illegittimo e migliorando la qualità dei dati trasmessi.

Invece, per l'eventuale utilizzo di Entratel, ovvero altro canale telematico, il Garante ha previsto che debbano essere introdotti da parte dell'Agenzia misure e accorgimenti volti ad assicurare innanzitutto che l'operatore finanziario possa inviare il *file*, già cifrato all'origine, in un'unica soluzione e che venga effettuata la certificazione digitale delle postazioni *client*, verificando la sicurezza delle postazioni periferiche. L'Agenzia dovrà prendere in considerazione, poi, l'utilizzo di strumenti *software* integrativi, idonei a rilevare altre qualità inerenti la sicurezza (ad es., aggiornamento dei sistemi di antivirus). Per l'autenticazione devono, inoltre, essere utilizzati sistemi di autenticazione informatica basati su tecniche di *strong authentication*, anche differenti e alternative rispetto all'utilizzo della Carta nazionale dei servizi.

Il Garante ha richiesto quindi all'Agenzia la separazione tra i profili di autorizzazione, consentendone una più completa e flessibile gestione, anche offrendo l'accesso in rete all'applicazione quantomeno su indirizzi o porte diverse da quelli utilizzabili in qualità di privato cittadino.

Per quanto attiene al trattamento posto in essere dagli operatori finanziari finalizzato alla comunicazione dei dati il Garante salva l'ipotesi dell'interconnessione *application-to-application* tra i rispettivi sistemi informativi ha disposto, in particolare, l'introduzione di meccanismi di

cifratura e di sicurezza già in fase di estrazione dei dati (finalizzati sia a proteggere le informazioni contenute nel *file* durante i successivi passaggi prima dell'invio all'Agenzia, che ad assicurare l'integrità del contenuto e a prevenirne alterazioni), la limitazione dell'accesso ai *file* ad un numero ristretto di incaricati, l'aggiornamento costante dei sistemi operativi, i *software* antivirus e antintrusione, l'eventuale conservazione dei dati solo in forma cifrata nonché, la fornitura dei *file* già cifrati ai responsabili o incaricati del trattamento.

Il Garante ha poi richiesto all'Agenzia di specificare nel provvedimento i tempi di conservazione dei dati presso l'Anagrafe tributaria e, una volta scaduti, di disporne la cancellazione automatica.

Con riferimento all'elaborazione delle liste selettive di contribuenti a maggior rischio di evasione, sulla base dei criteri successivamente individuati con provvedimento del Direttore dell'Agenzia il Garante, rilevato che l'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente, soprattutto se basati sulle numerose tipologie di dati contenute in Anagrafe tributaria, presenta rischi specifici per i diritti fondamentali, la libertà, e dignità degli interessati, ha ritenuto necessario che l'Agenzia gli sottoponga il menzionato provvedimento in sede di verifica preliminare al fine di prevedere adeguate garanzie per gli interessati medesimi (artt. 14 e 17 del Codice).

Nell'ottobre 2012, l'Agenzia delle entrate ha sottoposto all'esame del Garante un nuovo schema di provvedimento volto a regolare le modalità della comunicazione integrativa annuale all'archivio dei rapporti finanziari, che ha tenuto conto delle osservazioni e delle richieste avanzate dall'Autorità, nel menzionato parere del 17 aprile 2012 [doc. web n. 1886775].

Il nuovo schema prevede che i dati vengano trasmessi attraverso una nuova infrastruttura, il "Sistema di interscambio dati" -e non più con il servizio Entratel inizialmente individuato- le cui caratteristiche, attraverso il modulo *software open Java* per il controllo formale, la compressione e la cifratura dei dati da trasmettere, consentono di automatizzare il processo di raccolta dei dati presso gli operatori finanziari, riducendo i passaggi manuali tra incaricati del trattamento che aumentano di per sé le possibilità di accessi non autorizzati e trattamenti illegittimi. Banche e operatori finanziari dovranno quindi utilizzare due modalità alternative di intercambio informatizzato con il nuovo sistema: o un *server* Ftp, cioè un "nodo" di

colloquio con l'Agenzia, o il servizio di Posta elettronica certificata (Pec), utilizzabile in caso di *file* di piccole e medie dimensioni.

La predisposizione dei *file* da trasmettere all'Agenzia dovrà essere effettuata esclusivamente dall'operatore finanziario che non potrà avvalersi di intermediari fiscali.

Tuttavia, poiché l'architettura del sistema non è in grado di escludere eventuali interventi umani (in particolare, nelle operazioni di estrazione dei dati dai sistemi informativi, nonché nella ricezione delle ricevute, soprattutto presso operatori di medie-piccole dimensioni) e prevede la possibilità di passaggi intermedi (nodi di interscambio consorziati) nell'esprimere parere favorevole, il Garante ha chiesto l'adozione di alcune misure di sicurezza, innanzitutto prevedendo che il protocollo Ftp utilizzato per l'intercambio dei dati sia cifrato. L'Autorità ha, inoltre, individuato un'articolata serie di misure, analoghe a quelle già individuate nel citato provvedimento del 17 aprile 2012, che l'Agenzia e gli operatori finanziari dovranno adottare per minimizzare i rischi di accessi abusivi e trattamenti non consentiti e che, per quanto riguarda gli operatori finanziari, dovranno essere inserite nel testo del provvedimento dell'Agenzia. Nel prescrivere queste misure, il Garante ha tenuto conto delle esigenze dei piccoli operatori che non riescono ad automatizzare completamente la procedura e delle ipotesi in cui si avvalgano di nodi di interscambio esterni.

Inoltre l'Agenzia ha previsto che i dati non potranno essere conservati per più di sei anni, allo scadere dei quali saranno automaticamente cancellati.

L'Autorità si è comunque riservata di verificare nel dettaglio il completamento delle funzionalità della nuova infrastruttura informatica, anche prima della messa in esercizio.

Per quanto riguarda infine il provvedimento del Direttore dell'Agenzia con il quale saranno individuati i criteri per la formazione delle liste selettive dei contribuenti a maggior rischio di evasione, l'Agenzia ha dichiarato che sarà sottoposto preventivamente al Garante. L'Autorità ha in ogni caso stabilito che la verifica preliminare sia necessaria per ogni ulteriore utilizzo dei dati ad altre finalità (es. controlli Isee) (parere 15 novembre 2012 [doc. web n. 2099774]).

In seguito, l'Agenzia delle entrate ha rappresentato di voler utilizzare, in luogo della cifratura del protocollo Ftp, (utilizzato per lo scambio dei dati) prescritta dal Garante nel citato parere del 15 novembre 2012, la tecnologia VPN in modalità *site to site*, che assicura la

protezione del canale trasmissivo, su cui viaggiano in chiaro i soli parametri per l'apertura del canale stesso e i comandi Ftp. Il Garante, ritenendo così garantiti livelli di sicurezza non inferiori a quelli derivanti dalla cifratura del protocollo Ftp, ha consentito l'utilizzo di tale tecnologia nei termini prospettati. L'Autorità, inoltre, ha valutato positivamente la scelta dell'Agenzia di introdurre la firma dei *file* anche per le comunicazioni effettuate tramite Pec dagli operatori finanziari (provv. 31 gennaio 2013 [doc. web n. 2268436]).

Partecipazione dei comuni alla lotta all'evasione

L'Autorità ha dato parere favorevole a un schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità tecniche di accesso alle banche dati, di trasmissione di copia delle dichiarazioni relative ai contribuenti e la partecipazione all'accertamento fiscale e contributivo da parte dei comuni, in attuazione della normativa di settore (v. art. 1 del d.l. 30 settembre 2005, n. 203 convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248 e successive modificazioni) (provv. 17 aprile 2012 [doc. web n. 1886825]).

In particolare, il testo, d'intesa con la Guardia di finanza, l'Inps, l'Agenzia del territorio e la Conferenza unificata -fermo restando quanto stabilito dai provvedimenti del Direttore dell'Agenzia delle entrate del 7 dicembre 2007 e del 26 novembre 2008, entrambi sottoposti all'attenzione del Garante (cfr. rispettivamente, pareri 25 luglio 2007 [doc. web n. 1428047] e 30 ottobre 2008 [doc. web n. 1571156])- individua le ulteriori materie per le quali i comuni partecipano all'accertamento fiscale e contributivo e le modalità di accesso alle banche dati.

Il Garante ha espresso parere favorevole su tale schema a condizione che sia integrato al fine di garantire -per tutti i soggetti coinvolti nel trattamento- *standard* di sicurezza minimi non inferiori a quelli garantiti dall'Agenzia delle entrate in conformità al citato provvedimento del 18 settembre 2008.

Nel caso i comuni decidano di avvalersi di eventuali organismi esterni, questi devono essere preventivamente designati quali responsabili del trattamento. I comuni devono fornire adeguate istruzioni in merito al trattamento da effettuare e devono vigilare tramite verifiche periodiche, anche a campione. Qualora tali soggetti siano designati responsabili da più comuni, devono essere garantite misure di carattere tecnico organizzativo volte ad assicurare, nel rispetto degli ambiti territoriali comunali, la separazione logica dei dati e delle banche

dati trattati per conto dei diversi titolari, senza consentire la correlazione tra informazioni di competenza di ciascun comune.

In relazione, invece, alle modalità tecniche di accesso alle banche dati e a quelle di partecipazione dei comuni all'accertamento fiscale e contributivo di competenza, rispettivamente, dell'Agenzia del territorio e dell'Inps, il Garante ha richiesto un'integrazione dello schema che deve essere pertanto sottoposto nuovamente al parere dell'Autorità.

Riscossione

Con riferimento ai trattamenti di dati effettuati a fini di riscossione, il Garante ha prorogato al 30 giugno 2012, su richiesta di Equitalia in accordo con l'Agenzia delle entrate, alcuni degli adempimenti previsti dal provvedimento del 7 ottobre 2009 [doc. web n. 1664231], relativi all'articolazione delle diverse banche dati utilizzate a fini di riscossione, al reperimento delle informazioni anagrafiche da parte delle società del gruppo (a condizione che gli accessi alle anagrafi della popolazione residente effettuati dagli agenti della riscossione avvengano solo in presenza di una iscrizione a ruolo e mediante collegamenti realizzati nel rispetto di idonee misure di sicurezza) e alla predisposizione di attività di controllo, anche attraverso la realizzazione di appositi applicativi, sull'attività svolta dalle società controllate e da Sogei S.p.A. (provv. 12 maggio 2011 [doc. web n. 1822318]).

Secondo quanto rappresentato da Equitalia, infatti, la razionalizzazione dei sistemi informativi e la realizzazione di un nuovo sistema della riscossione hanno richiesto una rimodulazione dei tempi nel conseguimento degli obiettivi, anche in considerazione delle sostanziali modifiche normative intervenute nel 2010 che hanno imposto interventi di aggiornamento significativi. Di conseguenza, anche il processo di monitoraggio statistico di accesso al sistema deve essere riprogrammato con analoga scadenza stante la diretta subordinazione di tale adempimento con quello relativo alla razionalizzazione delle banche dati.

Nel 2012 Equitalia ha quindi dato conto al Garante di aver attuato il complesso processo di riorganizzazione societaria del gruppo, consolidando contestualmente l'infrastruttura tecnologica attraverso il completamento della procedura per la realizzazione di un sistema unico con conseguente razionalizzazione e unificazione delle basi dati. Con riferimento al reperimento delle informazioni anagrafiche da parte delle società del gruppo, Equitalia ha precisato che il nuovo regolamento di gestione dell'Indice nazionale delle anagrafi (decreto

del Ministro dell'interno del 19 gennaio 2012, n. 32), con cui sono state ampliate le informazioni al fine di rendere disponibili alle pp.aa. ulteriori dati anagrafici necessari per l'attività istituzionale, consente di disporre di informazioni complete, attuali e pertinenti. In relazione, invece, alla predisposizione di attività di controllo, il Garante, su richiesta di Equitalia, ha differito al 30 giugno 2013 il termine per gli adempimenti prescritti con il citato provvedimento del 2009, in considerazione dei tempi di progettazione e di avvio della fase sperimentale dei sistemi applicativi di supporto alle attività di controllo (provv. 12 luglio 2012 [doc. web n. 1913804]).

Agenzia delle dogane

L'Agenzia delle dogane ha comunicato all'Autorità l'intenzione di stipulare con l'Unità di informazione finanziaria (Uif) un protocollo che preveda la collaborazione e lo scambio di dati per l'esercizio delle rispettive funzioni istituzionali in materia di controllo sul denaro contante ai sensi del d.lgs. n. 195 del 2008.

In particolare, tale protocollo prevede che l'Agenzia consenta all'Uif, sulla base di specifiche richieste, di accedere alla banca dati relativa ai soggetti che hanno dichiarato trasferimenti di denaro contante.

Con specifico riferimento alle modalità tecniche di scambio di dati tra le autorità competenti, il Garante ha evidenziato che, oltre alle misure minime di sicurezza previste dal Codice, i titolari del trattamento sono tenuti ad adottare misure di sicurezza volte a ridurre al minimo, in particolare, gli accessi non autorizzati o i trattamenti non consentiti e non conformi alle finalità della raccolta.

Pertanto le amministrazioni coinvolte sono state invitate sia ad adottare misure che consentano gli accessi alla banca dati soltanto tramite postazioni di lavoro appartenenti alla rete *Ip* dell'ente autorizzato o/e dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'Agenzia, sia a rendere doverosa l'indicazione da parte dell'operatore dell'Uif del procedimento amministrativo alla base della specifica richiesta. Deve, inoltre, essere predefinita un'idonea procedura per il rilascio e la gestione delle credenziali di autenticazione e delle autorizzazioni con particolare riferimento alla tempestiva disabilitazione degli utenti. La *password*, da comunicare al singolo incaricato separatamente rispetto al codice di identificazione, deve essere modificata dallo stesso al

primo utilizzo e poi periodicamente, bloccando l'utenza a fronte di reiterati tentativi falliti di autenticazione. Le amministrazioni devono poi assicurare l'aggiornamento dei sistemi *software*, dei programmi utilizzati e della protezione antivirus, sia sui *server* che sulle postazioni di lavoro ed introdurre meccanismi volti a garantire che gli accessi avvengano esclusivamente nell'ambito di intervalli temporali o di data predeterminati, definiti sulla base delle esigenze d'ufficio, disciplinando la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone però l'utilizzo ai soli casi necessari per esigenze di servizio. In ogni caso, le operazioni di trattamento dei dati devono essere tracciate e devono essere stabilite periodiche verifiche sugli accessi (nota 26 giugno 2012).

4.6. SISTEMI DI VIDEOSORVEGLIANZA E *RFID* IN AMBITO PUBBLICO

Con riferimento al trattamento di dati personali tramite sistemi di videosorveglianza in ambito pubblico, l'Autorità ha ricevuto numerose segnalazioni, reclami e quesiti in ordine all'applicazione del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (punto 3.2. [doc. web n. 1712680]). Al riguardo molti comuni per disciplinare le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio hanno emanato uno specifico provvedimento, poi trasmesso al Garante per l'approvazione o solo per opportuna conoscenza. Al riguardo l'Autorità ha ribadito che l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo del Garante -fatte salve specifiche ipotesi- e che non può desumersi alcuna approvazione implicita dal semplice inoltro di documenti relativi a progetti di videosorveglianza, cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio assenso. L'Autorità ha inoltre informato i predetti comuni che l'Associazione nazionale comuni italiani (Anci) ha predisposto, con la collaborazione del Garante, linee-guida per fornire alcuni chiarimenti agli enti locali intenzionati ad attivare impianti di videosorveglianza nel territorio (*ex multis* note 7 giugno, 13 settembre, 7 dicembre 2011, 18 ottobre, 29 ottobre, 21 novembre e 20 dicembre 2012).

Più in dettaglio, con reclamo è stato rappresentato che un comune aveva conservato le immagini rilevate tramite un sistema di videosorveglianza per un periodo molto superiore alla

settimana, in quanto aveva potuto fornire nel 2010 ai Carabinieri che le avevano richieste nello svolgimento di indagini di polizia giudiziaria, immagini rilevate nel 2009. Al riguardo, l'Ufficio ha preliminarmente ribadito che la rilevanza e l'ammissibilità in giudizio di atti e documenti basati sul trattamento di dati non conforme alle norme vigenti restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (160, comma 6, del Codice). Con specifico riferimento alla questione oggetto del reclamo, l'Ufficio ha riscontrato invece l'inosservanza del provvedimento generale in materia di videosorveglianza del 29 aprile 2004 [doc. web n. 1003482] -vigente al tempo dei fatti contestati- che limitava ad una settimana la conservazione dei dati personali raccolti (cfr. punto 3.4.) ma non ha ravvisato i presupposti per adottare un provvedimento prescrittivo o inibitorio del Collegio, in quanto la condotta aveva esaurito i suoi effetti ed il comune titolare del trattamento aveva fornito idonee assicurazioni con riferimento alla funzionalità del sistema per cancellare le immagini tramite sovrascrittura delle stesse. In ragione della riscontrata condotta non conforme alla disciplina applicabile sono stati, comunque, avviati gli opportuni accertamenti per l'eventuale contestazione, con un autonomo procedimento sanzionatorio, della violazione amministrativa dell'inosservanza di provvedimenti prescrittivi del Garante (artt. 154, comma 1, lett. *c)* e 162, comma 2-*ter*, del Codice) (nota 26 gennaio 2012).

L'Autorità ha inoltre, ricevuto talune richieste di verifica preliminare alla luce delle indicazioni fornite nel predetto provvedimento generale (punto 3.2.) in particolare il Comune di Firenze ha chiesto la verifica preliminare, ai sensi dell'art. 17 del Codice, con riferimento al trattamento di dati personali relativo al sistema di videosorveglianza cd. "intelligente" che intendeva installare, per finalità di sicurezza urbana, presso la Fontana del Nettuno in Piazza della Signoria, oggetto nel corso degli anni di ripetuti atti vandalici, con ingenti danni al patrimonio pubblico. Tale sistema di videosorveglianza poteva rilevare le coordinate degli oggetti in movimento all'interno della superficie interdetta (consistente nella superficie e colonna d'aria sovrastante la fontana, il verde di bordura e la ringhiera che la circonda), azionare allarmi ottici e visivi individuando e, eventualmente, rilevando i percorsi delle persone e degli oggetti presenti all'interno dell'area stessa. Le immagini rilevate venivano registrate automaticamente in un *server* e conservate per un periodo di sette giorni.

L'Ufficio ha ritenuto corretta la richiesta verifica preliminare trattandosi di sistema di videosorveglianza cd. "intelligente", che non si limita a riprendere e registrare le immagini, ma rileva automaticamente comportamenti o eventi anomali, li segnala e, eventualmente, registra (punto 3.2.1. provv. 8 aprile 2010 [doc. web n. 1712680]). In tale quadro l'Ufficio ha anche rilevato che il trattamento in parola rientra nelle funzioni istituzionali del comune cui spettano specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana per la tutela della quale gli stessi possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico (cfr. art. 54, d.lgs 18 agosto 2000, n. 267; d.m. 5 agosto 2008; art. 6, comma 7, d.l. 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla l. 23 aprile 2009, n. 38). L'Ufficio, alla luce delle motivazioni addotte dal Comune, ha ritenuto proporzionato e ammissibile il trattamento per il rischio del protrarsi degli atti vandalici e dell'elevato valore artistico del monumento, richiamando comunque l'attenzione del Comune stesso sugli adempimenti relativi alle misure di sicurezza ed all'informativa agli interessati (cfr. punto 3.3.1. del cit. provvedimento generale; artt. 13, 31 e 36 del Codice e Allegato B. al Codice) (provv. 7 aprile 2011 [doc. web n. 1811897]).

Ad una provincia che chiedeva se fosse necessario sottoporre alla verifica preliminare un sistema di videosorveglianza da installare presso il palazzo provinciale, l'Ufficio ha evidenziato che spetta alla singola amministrazione valutare se i trattamenti di dati siano riconducibili a quelli che, in base al provvedimento generale, richiedano la verifica preliminare (punto 3.2.1. del cit. provvedimento; art. 17 del Codice) (nota 29 ottobre 2012).

È stato, invece, correttamente sottoposto alla verifica preliminare un sistema di videosorveglianza installato in taluni musei dipendenti dalla Soprintendenza per i beni archeologici di una regione, con riferimento all'intenzione di allungare a trenta giorni i tempi di conservazione delle immagini raccolte, come richiesto dal Comando Legione dei Carabinieri, in considerazione della recrudescenza dei reati contro il patrimonio e dei trafugamenti di opere d'arte. In base agli elementi forniti e alle valutazioni del Comando dei Carabinieri il periodo è stato ritenuto congruo in quanto rispettoso del principio di proporzionalità ma l'allungamento è stato limitato al permanere di tale eccezionale necessità (provv. 18 ottobre 2012 [doc. web n. 2138277]).

Ancora sull'allungamento dei tempi di conservazione delle immagini, l'Ufficio ha precisato a due soggetti pubblici che volevano conservare le immagini registrate, rispettivamente per 5 e 2 giorni, che in base al provvedimento generale del 2010 spetta al titolare del trattamento valutare la sussistenza dei presupposti, quali le peculiari esigenze tecniche o la particolare rischiosità dell'attività, che giustificano la conservazione delle immagini raccolte per un periodo di tempo superiore alle ventiquattro ore e comunque inferiore alla settimana. La verifica preliminare deve essere richiesta al Garante solo se i tempi di conservazione superano una settimana (note 5 e 20 dicembre 2012).

Sempre nell'ambito delle richieste di verifica preliminare, si menziona quella di un comune relativa ad un sistema di videosorveglianza cd. "intelligente" -fornito da una università- per la rilevazione e la segnalazione agli operatori, in maniera automatica e in tempo reale, di eventi critici in alcune aree ritenute sensibili.

Nell'ambito della prima fase del progetto un gruppo di ricerca dell'università si sarebbe occupato di sperimentare, collegandosi al sistema di videosorveglianza cittadino, un applicativo per il rilevamento mediante analisi visuale della presenza di folle, utilizzando unicamente immagini relative ad attori consenzienti. Il comune aveva, quindi, formulato un quesito all'Autorità sulla necessità di sottoporre a verifica preliminare il trattamento dei dati personali di questa prima fase del progetto, precisando che la realizzazione della seconda fase (caratterizzata dall'implementazione delle telecamere intelligenti nel sistema di videosorveglianza cittadino e dall'attivazione delle stesse nelle zone ritenute particolarmente sensibili) sarebbe stata, in ogni caso, preceduta dalla richiesta di verifica preliminare al Garante.

L'Ufficio, nel rispondere al comune, ha evidenziato che essendo nella prima fase il sistema di videosorveglianza intelligente non ancora definito, l'Autorità non era nelle condizioni di individuare idonee misure ed accorgimenti a garanzia degli interessati, non essendo possibile valutare in concreto i rischi del trattamento per i diritti e la dignità degli interessati, in relazione alla specifica finalità perseguita ed al contesto in cui i dati vengono trattati. Pertanto la verifica preliminare è stata ritenuta non necessaria in relazione alla prima fase del progetto.

Essa sarà, invece, necessaria nella seconda fase, poiché al termine della sperimentazione l'Autorità sarà nelle condizioni di valutare gli effetti prodotti dal sistema di videosorveglianza

in relazione, in particolare, alle specifiche finalità perseguite e al contesto in cui il trattamento avrà luogo; elementi, questi ultimi, che il comune dovrà opportunamente evidenziare nell'ambito della predetta richiesta (cfr. punto 3.2.1. provv. 8 aprile 2010, pubblicato in G.U. 29 aprile 2010, n. 99 [doc. web n. 1712680]). Tali indicazioni, fornite dall'Ufficio, sono state sottoposte all'esame del Collegio (nota 22 novembre 2012).

Non è mancata occasione, anche nel 2012, di fornire chiarimenti in merito all'installazione di sistemi di videosorveglianza presso gli istituti scolastici, in particolare in relazione alla lamentata attivazione continua di telecamere all'interno di un istituto e del relativo convitto.

Al riguardo, l'Ufficio ha richiamato il provvedimento dell'8 aprile 2010, nel quale è stata ribadita la necessità di garantire il diritto dello studente alla riservatezza (art. 2, comma 2, d.P.R. n. 249/1998), prevedendo opportune cautele per assicurare l'armonico sviluppo della personalità dei minori. È stato, altresì, evidenziato che può risultare ammissibile l'utilizzo di sistemi di videosorveglianza in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate, attivando gli impianti negli orari di chiusura degli istituti e vietando la messa in funzione delle telecamere in coincidenza con lo svolgimento di eventuali attività *extra*-scolastiche che si svolgono all'interno della scuola (punto 4.3.1. cit. provv.).

Nelle medesime circostanze, è stato inoltre chiarito che la ripresa di immagini delle aree perimetrali esterne degli edifici scolastici deve essere delimitata alle sole parti interessate, escludendo le aree non strettamente pertinenti l'edificio (punto 4.3.2.); il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (nota 20 dicembre 2012).

È stato altresì ricordato il divieto di controllo a distanza dell'attività lavorativa. Sono infatti vietate l'installazione di apparecchiature preordinate alla predetta finalità nonché le riprese miranti a verificare l'osservanza dei doveri di diligenza e la correttezza nell'esecuzione della prestazione lavorativa (ad es., orientando la telecamera sul *badge*). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature "*dai quali può*

derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lgs. n. 165/2001) (punto 4.1. cit. provv.).

Rfid

Un'altra verifica preliminare è stata richiesta da un comune in relazione al trattamento di dati personali effettuato attraverso un sistema *Rfid (Radio frequency identification*), per la rilevazione degli orari di ingresso e di uscita dalla zona a traffico limitato (ztl) dei veicoli adibiti al trasporto delle merci per sanzionare i veicoli che si trattengono all'interno della predetta zona oltre l'orario consentito.

Il sistema *Rfid* usa onde elettromagnetiche per l'identificazione automatica di cose o persone, ed è composto di un *tag* (cioè di un'etichetta, dispositivo elettronico di memoria con un codice identificativo unico) e di un lettore utilizzato per leggere tali informazioni. Il Garante con il provvedimento generale del 9 marzo 2005 [doc. web n. 1109493] aveva già individuato specifiche garanzie per l'uso delle cd. "etichette intelligenti" (*Rfid*), riservandosi di prescrivere la verifica preliminare solo per i sistemi *Rfid* destinati all'impianto sottocutaneo.

Il sistema in esame si compone di un'antenna posta su un palo collegata ad una piccola unità locale che registra solo il numero delle targhe dei veicoli autorizzati all'accesso alla ztl, associate al codice univoco con cui il *tag* è identificato dal produttore. Il sistema avrebbe dovuto essere attivo 24 ore su 24, per registrare i *tag* (ingresso e uscita) e consentire di penalizzare i veicoli usciti dalla ztl oltre l'orario consentito. L'Ufficio non ha ritenuto necessaria la verifica preliminare, a garanzia dei diritti degli interessati (art. 7, comma 1, lett. *g),* del codice della strada), ma ha prescritto, in particolare, che l'informativa (art. 13 del Codice) sia resa all'atto della richiesta del permesso, prima dell'istallazione del sistema *Rfid* sui veicoli autorizzati e, comunque, prima della sua attivazione. Inoltre, in osservanza del principio di necessità (art. 3 del Codice), ha disposto che l'identificazione degli interessati tramite la targa possa essere effettuata solo per l'accertamento della violazione delle regole concernenti gli orari di ingresso e di uscita dalla ztl dei veicoli in parola e per l'applicazione della relativa

sanzione. Con riferimento, poi, ai tempi di conservazione (v. art. 11, comma 1, lett. *e)*, del Codice), il Garante ha prescritto di cancellare le informazioni relative ai veicoli entrati ed usciti dalla ztl nei tempi consentiti subito dopo l'uscita e, in caso di infrazione, di conservare le informazioni rilevate per il solo periodo necessario alla contestazione dell'infrazione stessa, all'applicazione dalla sanzione e alla definizione dell'eventuale contenzioso. Sono state, infine, fornite specifiche indicazioni per garantire la sicurezza dei dati trattati (provv. 2 febbraio 2012 [doc. web n. 1875840]).

4.7. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

L'applicazione della disciplina in materia di protezione dei dati personali in ambito locale e regionale continua a presentare profili problematici.

In relazione alla segnalazione di un'associazione che lamentava una presunta violazione del Codice da parte di una provincia nel quadro di un cd. "Piano territoriale per l'immigrazione" -volto a garantire l'inserimento sociale dei migranti- l'Ufficio ha accertato che non erano mai stati raccolti dati sensibili e le associazioni coinvolte nel progetto venivano correttamente designate responsabili del trattamento. Pertanto non è stata intrapresa alcuna iniziativa (nota 18 ottobre 2012).

Un ulteriore caso ha riguardato l'accesso *online* alla Banca dati dell'emergenza (Bde) istituita dal Comune dell'Aquila, in cui ogni residente può controllare la sua posizione relativamente all'assistenza e alla ricostruzione *post* sisma, tramite l'inserimento di *user id* e *password* individualmente assegnate, previa registrazione con il solo inserimento delle proprie generalità e codice fiscale. L'Ufficio ha rappresentato che per consentire l'accesso ai servizi erogati in rete dal Comune, è necessario l'utilizzo della carta d'identità elettronica e della carta nazionale dei servizi, ovvero di strumenti diversi, purché idonei a consentire l'individuazione informatica del soggetto che richiede il servizio (art. 64, commi 1 e 2, d.lgs. 7 marzo 2005, n. 82). A seguito delle assicurazioni fornite dal Comune relativamente alle procedure di accredito, affinché la consultazione della singola posizione presente in Bde sia univocamente effettuata dall'interessato, l'Ufficio non ha adottato alcun provvedimento (nota 10 dicembre 2012).

Il Garante è stato inoltre interpellato da un comune in ordine alla possibilità di acquisire dagli albergatori -previa adozione di un regolamento per disciplinare il flusso dei dati- le generalità dei turisti che rifiutano di corrispondere la cd. "tassa di soggiorno". Al riguardo l'Ufficio ha chiarito che per la comunicazione non è necessario il consenso degli interessati in presenza di un obbligo stabilito da norme vigenti, ivi compresi i regolamenti (art. 24, comma 1, lett. *a)*, del Codice) (nota 23 agosto 2012).

Sotto un diverso profilo, una cittadina lamentava che il comune di residenza, per emettere la nuova tessera elettorale in sostituzione di quella vecchia priva di spazi per la certificazione del voto, aveva richiesto la restituzione del documento. L'Autorità, considerando che la tessera, riportando l'annotazione della partecipazione al voto, è in grado di rivelare il comportamento elettorale di una persona e, in alcuni casi, l'orientamento politico, ha evidenziato le ragioni della segnalante ed interessato della vicenda il Ministero dell'interno, che ha dato disposizioni alle proprie strutture periferiche di non procedere più in tali casi al ritiro del documento. Questo anche alla luce della normativa in materia, che prevede la restituzione della tessera solo in un numero limitato di ipotesi, tra le quali non rientra l'esaurimento degli spazi per le timbrature (nota 23 agosto 2012).

In un altro caso è stato segnalato che presso il cd. "Sportello unico" per il cittadino di un comune non venivano rispettate le garanzie previste dalla legge a tutela della dignità e della riservatezza delle persone. L'Ufficio ha ribadito al comune che i titolari del trattamento devono a tal fine adottare idonei accorgimenti (cfr. artt. 29 e 30 del Codice), tra i quali, per prevenire l'accesso anche "passivo" ai dati da parte di terzi non autorizzati (ad es., da parte di uno dei componenti la "fila"), l'opportuna istituzione della cd. "distanza di cortesia"(nota 13 dicembre 2012).

In un'altra vicenda, un cittadino ha segnalato che un comune aveva notificato all'interessato una comunicazione in materia urbanistica omettendo di adottare le opportune cautele a tutela della riservatezza, in quanto l'atto in questione non era stato consegnato in mani proprie del destinatario, bensì era stato recapitato a un vicino di casa senza essere inserito in busta sigillata, in violazione dell'art. 174 del Codice. Il comune ha rappresentato che il messo notificatore aveva depositato la comunicazione nell'apposita cassetta delle lettere

dell'interessato e che ignorava come la comunicazione potesse essere finita nella mani di un soggetto estraneo alla procedura.

L'Ufficio, non ravvisando gli estremi di una violazione della disciplina di protezione dati, ha comunque inviato il comune a verificare il rispetto delle citate disposizioni in materia di notificazioni degli atti (nota 25 settembre 2012).

In un altro caso, l'interessato lamentava l'avvenuta notifica a un suo congiunto di una nota con cui si intimava il pagamento dei costi sostenuti dal comune per il ricovero dell'interessato stesso presso strutture assistenziali. Avendo rilevato l'avvenuta comunicazione di dati idonei a rivelare lo stato di salute dell'interessato a terzi, l'Ufficio si è riservato, con autonomo procedimento, di verificare i presupposti per contestare la violazione amministrativa concernente la illegittima comunicazione di dati personali (art. 162, comma 2-*bis*, per violazione dell'art. 20, comma 2, del Codice) (nota 10 dicembre 2012).

Un'altra segnalazione evidenziava che nella documentazione fotografica inviata da un comune a corredo della contestazione di violazione del codice della strada risultavano visibili anche soggetti estranei all'accertamento. Alla luce del provvedimento in materia di videosorveglianza (provv. 8 aprile 2010 [doc. web n. 1712680], in G.U. 29 aprile 2010, n. 99; cfr. Relazione 2009 p. 25 e ss.) in cui è stabilito che la ripresa non deve comprendere soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada), nonché sulla base delle direttive emanate dal Ministero dell'interno, l'Autorità ha prescritto al comune di mascherare per il futuro la porzione delle risultanze video/fotografiche riguardante i soggetti estranei allo specifico accertamento amministrativo (cfr. artt. 143, comma 1, lett. *b)*, e 154, comma 1, lett. *c)*, del Codice). Inoltre, ha vietato al segnalante ogni eventuale trattamento dei dati personali di soggetti non coinvolti nell'accertamento amministrativo, contenuti nella documentazione fotografica speditagli illecitamente dal comune (artt. 143, comma 1, lett. *c)* e 154, comma 1, lett. *d)*, del Codice) (provv. 13 dicembre 2012 [doc. web n. 2185265]).

Si evidenzia, inoltre, il riproporsi di tematiche inerenti il trattamento dei dati da parte di soggetti esterni all'amministrazione comunale, per l'esercizio di funzioni istituzionali (*outsourcing*). In particolare, è stato segnalato che un comune aveva affidato il servizio di noleggio degli autovelox, nonché la gestione delle relative procedure sanzionatorie, a una

società esterna che, a sua volta, aveva affidato a terzi la stampa, l'imbustamento e la spedizione dei verbali di infrazione. In merito, il Garante ha in particolare rappresentato l'esigenza che l'amministrazione -in qualità di titolare del trattamento- designi il soggetto esterno preposto al trattamento come "responsabile del trattamento" con apposito atto scritto che specifichi analiticamente i compiti affidatigli (art. 29 del Codice). In caso contrario, il trattamento di dati personali si configura come una comunicazione esterna, assoggettata alle più stringenti norme previste per tale operazione (art. 19, comma 3, del Codice). Nel caso di specie è stato rappresentato che tutte le società che trattano dati personali per conto del comune dovevano essere nominate responsabili del trattamento da parte del comune e, quindi, anche il soggetto terzo indicato dalla società per l'imbustamento e la stampa dei verbali di infrazione (nota 30 luglio 2012).

4.7.1. Raccolta differenziata dei rifiuti solidi urbani

Nel 2012, il Garante è tornato nuovamente ad interessarsi del trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti solidi urbani.

In particolare, in relazione a tre segnalazioni, nel richiamare le prescrizioni contenute nel provvedimento generale del 14 luglio 2005 [doc. web n. 1149822], è stata esaminata la possibilità che vengano effettuate ispezioni generalizzate del contenuto dei sacchetti per identificare il presunto trasgressore delle prescrizioni relative alla raccolta differenziata dei rifiuti (tipologia di materiale da conferire, specifici giorni o orario di conferimento). Al riguardo è stato evidenziato che agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689), ma tale facoltà deve essere limitata ai soli casi in cui il soggetto non sia in altro modo identificabile. Risulterebbe, quindi, illegittima la pratica di ispezioni generalizzate da parte del personale incaricato, al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente.

La modalità di accertamento descritta può anche rivelarsi lesiva di situazioni giuridicamente tutelate come la libertà e la segretezza della corrispondenza lasciata nei rifiuti

ed inoltre non sempre risulta agevole, in base agli elementi in esso contenuti, provare la provenienza del sacchetto. Alla luce di tale considerazione si ritiene che il trasgressore non dovrebbe essere individuato sempre ed esclusivamente attraverso una ricerca nel sacchetto dei rifiuti di elementi (corrispondenza o altri documenti) a lui riconducibili, e che quindi una eventuale sanzione amministrativa irrogata ad un soggetto così individuato potrebbe risultare erroneamente comminata (cfr. punto 4. *d)* del citato provvedimento generale) (note 29 ottobre e 5 dicembre 2012).

4.8. COMUNICAZIONI DI DATI PERSONALI TRA SOGGETTI PUBBLICI

Per quanto riguarda la trasmissione di dati fra soggetti pubblici, il Garante ha espresso il parere sullo schema di Accordo tra Ministero della salute, enti locali, province e regioni, sulla prevenzione degli effetti delle ondate di calore, in particolare riguardo alla trasmissione alle Ausl, da parte delle amministrazioni comunali, degli elenchi aggiornati delle persone residenti di età pari o superiore ai 65 anni iscritte nelle anagrafi. Il Garante ha espresso parere favorevole alla trasmissione in quanto la normativa di settore prevede che l'ufficiale di anagrafe possa rilasciare, anche periodicamente, alle amministrazioni pubbliche "*che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità*" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223) elenchi degli iscritti nella Anagrafe della popolazione residente (art. 19, comma 2, del Codice) (provv. 18 maggio 2012 [doc. web n. 1900390]).

Sempre in tema di comunicazione di dati fra soggetti pubblici, si ricorda il caso di un comune che aveva comunicato all'Autorità l'intenzione di fornire indirizzi di residenti e proprietari di immobili, come risultanti dalla banca dati dell'Imposta comunale sugli immobili (Ici), alla soprintendenza per i beni architettonici e paesaggistici di una regione, che ne aveva fatto richiesta, per procedere alla verifica e rinotifica di dichiarazione di interesse culturale (artt. 19, comma 2, e 39, comma 1, del Codice). Al riguardo, alla luce della disciplina di settore (artt. 10 e ss., d.lgs. 22 gennaio 2004, n. 42, "Codice dei beni culturali e del paesaggio"), l'Ufficio non ha formulato osservazioni ostative. È stata comunque richiamata l'esigenza di rispettare i princìpi di pertinenza e di non eccedenza, sensibilizzando il comune in ordine all'esigenza di trasmettere alla suddetta soprintendenza

solo dati strettamente indispensabili per lo scopo istituzionale perseguito (art. 11 del Codice) (nota 8 novembre 2012).

Si segnala inoltre il quesito inoltrato da una Asl in ordine alla richiesta di accesso alla banca dati regionale dell'Anagrafe sanitaria presentata dal Comando Carabinieri-NAS. In merito, il Garante ha ribadito che "*la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia*" è consentita "*per finalità […] di prevenzione, accertamento o repressione di reati"* (art. 25, comma 2, del Codice). Tuttavia, l'acquisizione per via telematica di dati, informazioni, atti e documenti da parte delle forze di polizia, in conformità alle vigenti disposizioni di legge o di regolamento, rimane subordinata alla stipula di apposite "*convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei princìpi di cui agli articoli 3 e 11*" (art. 54, comma 1, del Codice). Tali *"convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'art. 53"* (art. 54, comma 1, del Codice). In mancanza della suddetta convenzione, la comunicazione dei dati richiesti, con modalità diverse da quella telematica, per esigenze di polizia giudiziaria dal Comando Carabinieri-NAS è possibile soltanto per i dati, pertinenti e non eccedenti, necessari alle finalità di volta in volta rappresentate dalle forze di polizia stesse (nota 27 marzo 2012) (per i pareri espressi dal Garante su alcune convenzioni-tipo; cfr. *infra* par. 8.2.1.).

4.8.1. Il nuovo sistema AVCPass

Il Garante ha espresso parere favorevole sulla deliberazione dell'Autorità per la vigilanza sui contratti pubblici (di seguito Avcp) attuativa dell'art. 6-*bis* del d.lgs. 12 aprile 2006, n. 163 (codice dei contratti pubblici relativi a lavori, servizi e forniture), in base al quale, dal 1° gennaio 2013, le stazioni appaltanti e gli enti aggiudicatori devono verificare il possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per la partecipazione alle procedure disciplinate dal citato codice dei contratti pubblici

esclusivamente tramite la Banca dati nazionale dei contratti pubblici (Bdncp), istituita presso l'Avcp medesima. Tale atto è volto ad individuare i dati da inserire nella Bdncp al fine di consentire alle stazioni appaltanti/enti aggiudicatori di verificare il possesso dei requisiti degli operatori economici per l'affidamento dei contratti pubblici; a istituire il nuovo sistema *AVCPass* (*Authority Virtual Company Passport*), finalizzato alla verifica *online* dei requisiti attraverso la Bdncp, dotato di apposite aree dedicate ad operatori economici e a stazioni appaltanti/enti aggiudicatori; a stabilire i termini e le regole tecniche per l'acquisizione, l'aggiornamento e la consultazione dei predetti dati.

Il testo tiene conto delle indicazioni fornite all'Avcp dall'Ufficio del Garante, riguardanti in particolare, le modalità di realizzazione dei flussi informativi previsti nell'ambito del sistema *AVCPass*, la definizione di misure di sicurezza idonee a garantire i rischi di accessi non autorizzati e di trattamenti non consentiti o non conformi alle finalità della raccolta.

Il parere favorevole del Garante è stato, infine, condizionato all'esplicitazione del tempo di conservazione dei dati relativi agli accessi e alle operazioni compiute nel sistema (parere 19 dicembre 2012 [doc. web n. 2171106]).

4.9. L'ATTIVITÀ GIUDIZIARIA

Sicurezza nelle intercettazioni

Con delibera del 13 settembre 2012 il Garante ha avviato gli accertamenti volti a verificare l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati svolti presso le procure della Repubblica, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attività di intercettazione di conversazioni o comunicazioni, effettuate per ragioni di giustizia, nonché preventive (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.).

Al fine di individuare modalità operative e di cooperazione più efficaci il Garante, in una prima fase, ha inoltrato una preliminare richiesta di informazioni volta ad acquisire da alcune procure di medie dimensioni, dislocate in diverse aree del territorio nazionale e che hanno sede presso capoluoghi di provincia, elementi conoscitivi utili all'espletamento dei successivi accertamenti da svolgere *in loco*.

Le procure interpellate hanno fornito le informazioni richieste, che sono all'esame dell'Autorità.

Anche nel 2012 sono pervenute segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo che prevede la pubblicazione in appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80).

Al riguardo con due segnalazioni veniva lamentata la pubblicazione, sui siti istituzionali di due tribunali, di avvisi d'asta che recavano, tra le altre informazioni, i nominativi delle persone intestatarie dell'immobile oggetto della vendita nonché, nel primo caso, diverse immagini nelle quali erano riconoscibili i soggetti esecutati e, nel secondo, il nome del defunto coniuge di una delle persone soggette ad esecuzione.

Svolte le necessarie verifiche, l'Autorità ha rappresentato ai presidenti dei tribunali che, negli avvisi di vendita, dev'essere omessa l'indicazione del debitore (art. 490, comma 3, c.p.c., come modificato dall'art. 174, comma 9, del Codice) e, con riferimento ai documenti generalmente allegati agli avvisi d'asta, ha ribadito che anche i trattamenti di dati personali effettuati per motivi di giustizia sono assoggettati ai princìpi sanciti dall'art. 11 del Codice, fra i quali il principio di pertinenza e non eccedenza (comma 1, lett. *d)*).

Alla richiesta di fornire riscontro in ordine alle determinazioni adottate, nel primo caso il giudice delegato ai fallimenti ha disposto che la società incaricata della pubblicazione degli avvisi d'asta sul sito del tribunale provvedesse all'oscuramento di tutti i dati personali identificativi relativi a soggetti a vario titolo coinvolti nelle procedure esecutive individuali e concorsuali presenti negli atti pubblicati *online* e ha altresì disposto l'oscuramento di tutti i dati personali relativi ai segnalanti. La società destinataria del provvedimento ha ottemperato al disposto dandone avviso al giudice delegato e al Garante.

Nel secondo caso il presidente del tribunale ha rappresentato che l'associazione notarile per le procedure esecutive ha predisposto che i professionisti che redigono gli avvisi di vendita forniscano al soggetto addetto alla pubblicità documenti già privi di ogni dato non pertinente. La società responsabile per la pubblicazione in internet ha confermato che l'avviso d'asta oggetto della segnalazione non era più reperibile in rete (note 2 dicembre 2011 e 27 settembre 2012).

Competenza in materia di trattamento dei dati di parlamentari da parte di un organo delle Camere

Alcuni parlamentari avevano presentato al Garante un reclamo nei confronti del Presidente del Consiglio di giurisdizione della Camera dei deputati che, durante una conferenza stampa che aveva avuto vasta eco sui mezzi di informazione, aveva rivelato i nomi dei deputati ed *ex* deputati che avevano presentato ricorso avverso una deliberazione dell'Ufficio di Presidenza della Camera che aveva introdotto norme restrittive del loro trattamento previdenziale.

Il Garante ha dichiarato inammissibili i reclami in quanto il Consiglio di giurisdizione, quale organo della Camera dei deputati, è espressione del potere di autodichia degli organi costituzionali, disciplinato dai relativi regolamenti, nell'ambito della sfera di autonomia riservata loro dalla Costituzione (art. 64, primo comma). In ragione di tale autonomia, il Codice prevede che i trattamenti di dati personali effettuati dagli organi costituzionali sono disciplinati dai medesimi organi in conformità ai rispettivi ordinamenti (art. 22, comma 12) e la deliberazione n. 208 del 26 ottobre 2004 dell'Ufficio di Presidenza della Camera, recante la "Normativa in tema di protezione dei dati personali", stabilisce che, in tale materia "*si applicano le norme relative alla tutela dinanzi agli organi di giurisdizione interna della Camera dei deputati"* (art. 4). Trattandosi di atti di autonomia normativa adottati dal Parlamento ai sensi dell'art. 64, primo comma, della Costituzione, i regolamenti sono sottratti ad ogni sindacato da parte di qualsiasi altro potere dello Stato (cfr. Corte cost., sentenza n. 154 del 1985; Corte europea dei diritti dell'uomo, *Affaire Savino et autres c. Italie;* sentenza del 28 aprile 2009; Cass. civ., sez. unite, sentenza n. 11019/2004) (nota 3 aprile 2012).

Contenuto del decreto di giudizio immediato *ex* art. 456 c.p.p.

È stato sottoposto all'Autorità un quesito in ordine alla conformità alla disciplina del Codice dell'inserimento del domicilio della persona offesa nei decreti di disposizione del giudizio immediato nei confronti dell'imputato, di cui all'art. 456 c.p.p.. Il Garante ha ricordato che in base alla normativa applicabile (art. 52 del Codice e art. 456 c.p.p.) l'indirizzo della persona offesa, ancorché non formalmente indicato quale requisito del decreto di fissazione del giudizio immediato, costituisce tuttavia un'informazione essenziale ai fini della necessaria notificazione del provvedimento, salvo il caso in cui la parte abbia un difensore (domiciliatario *ex lege*). La questione appare peraltro rivestire una rilevanza formale, in quanto sia il difensore dell'imputato -che può svolgere indagini difensive ai sensi degli

artt. 391-*bis* e ss. c.p.p.- sia lo stesso imputato personalmente, hanno il diritto di prendere visione di tutti gli atti del fascicolo delle indagini, dove sono riportate le generalità complete e l'indirizzo anche della persona offesa; pertanto, omettere l'indirizzo nella copia del decreto che viene notificata all'imputato e al suo difensore appare una precauzione sostanzialmente inutile, a fronte dei diritti e delle garanzie di difesa (nota 30 novembre 2012).

Astensione dall'incarico di un consulente tecnico d'ufficio

In ordine ad un presunto trattamento illecito dei dati personali effettuato da un consulente tecnico d'ufficio nella comunicazione al magistrato dei motivi di astensione dall'incarico, che il segnalante riteneva lesiva della propria riservatezza e dannosa per la propria posizione processuale, il Garante ha ritenuto legittima tale comunicazione, in quanto il consulente che intende astenersi deve farne denuncia o istanza al magistrato che gli ha conferito l'incarico, perché si valuti se ricorra un giusto motivo di astensione (art. 63 c.p.c., 192 disp. att. c.p.c.) (nota 8 ottobre 2012).

Banca di dati sanitari ed attività dell'autorità giudiziaria

Una procura della Repubblica ha posto al Garante un interessante quesito riguardante la fattibilità di un protocollo da stipularsi tra la procura stessa e alcuni enti pubblici competenti, a vario titolo, in materia sanitaria, per favorire l'emersione delle patologie oncologiche aventi un nesso con l'esposizione lavorativa, attraverso l'inserimento in una banca dati condivisa delle informazioni in possesso degli enti firmatari -quali generalità del malato, patologia, attività lavorativa prestata, mansioni svolte- ai fini dell'eventuale promozione, da parte dell'autorità giudiziaria, di procedimenti penali tesi all'accertamento di responsabilità penali.

Il Garante, pur apprezzando lo scopo dell'iniziativa, ha rilevato che appare dubbio che i trattamenti svolti per ragioni di giustizia, come normativamente definiti, comprendano l'acquisizione ed il monitoraggio preventivo e generalizzato dei dati personali di tutti i lavoratori affetti dalle malattie croniche dalle caratteristiche eziologiche sopra precisate, al fine di individuare eventuali ipotesi delittuose. Del resto, il Codice prevede che l'autorità giudiziaria possa acquisire atti e documenti da soggetti pubblici, anche per via telematica, solo in conformità alle vigenti disposizioni processuali (art. 48 del Codice), ma il protocollo non individua un'idonea base normativa, che non potrebbe rinvenirsi nella disciplina sui poteri di accertamento dei reati da parte del pubblico ministero che non legittimano un flusso indiscriminato di dati, soltanto alcuni dei quali potrebbero costituire *notitiae criminis*.

Secondo la giurisprudenza di legittimità, inoltre è da escludere che possano essere promosse indagini preliminari non già sulla base di una notizia di reato, ma al fine di eventualmente acquisirla, con indagini a tappeto e in forma indiscriminata, dirette ad accertare se eventualmente ipotetici reati sono stati commessi (Cass., sez. terza, sentenza n. 3261/1999).

D'altro canto, poiché il trattamento -quindi, anche la comunicazione- di dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge (art. 20 del Codice), gli enti partecipanti al progetto non possono conferire tali dati per autonoma e volontaria determinazione, non avendo la piena ed incondizionata disponibilità dei dati detenuti *ratione officii* essendo, invece, necessaria una specifica norma di legge -come nel caso del "Sistema informativo nazionale per la prevenzione nei luoghi di lavoro", previsto e disciplinato dall'art. 8 del d.lgs. 9 aprile 2008, n. 81- o una autorizzazione del Garante (nota 12 dicembre 2012).

Ordini di esibizione dell'autorità giudiziaria

Con riferimento al quesito di un istituto pubblico in relazione alle richieste inoltrate dall'autorità giudiziaria ai sensi dell'art 256 c.p.p. di esibizione o sequestro di dati coperti dal segreto statistico, il Garante ha rappresentato che in base al Codice (art. 108) il trattamento di dati personali effettuato per scopi statistici da parte di soggetti che fanno parte del Sistema statistico nazionale, resta disciplinato, oltre che dal codice di deontologia e di buona condotta (provv. 16 giugno 2004 [doc. web n. 1556635]), dal d.lgs. 6 settembre 1989, n. 322 il quale detta, tra l'altro, disposizioni per la tutela del segreto statistico e indica anche i dati che non sono coperti dal segreto (art. 9).

Spetta pertanto all'istituto verificare se i dati oggetto della richiesta dell'autorità giudiziaria rientrano tra quelli coperti dal segreto statistico, attenendosi, in quest'ultimo caso, a quanto prevede l'art. 256 c.p.p. (nota 9 febbraio 2012).

Richiesta del giudice civile di accesso ai tabulati telefonici

Un tribunale ha chiesto al Garante di esprimersi sulla legittimità del rifiuto, opposto da alcune società telefoniche, all'ordine di esibizione dei tabulati telefonici emanato, ai sensi dell'art. 210 c.p.c., nell'ambito di una controversia civile.

Il Garante ha ricordato che i dati relativi al traffico telefonico non più necessari ai fini della trasmissione della comunicazione elettronica sono cancellati o resi anonimi dal fornitore del servizio, al quale è consentito il trattamento a fini di fatturazione per un periodo non

superiore a sei mesi, salva l'ulteriore conservazione necessaria per effetto di una contestazione anche in sede giudiziale. Al di fuori di tali ipotesi, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, solo per finalità di accertamento e repressione di reati (art. 132 del Codice, commi 1 e 3), non per richieste formulate nell'ambito di una controversia civile, amministrativa e contabile (in tal senso v. provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008 [doc. web n. 1482111]).

Pertanto, il diniego opposto dalle società telefoniche all'ordine dell'autorità giudiziaria *ex* art. 210 c.p.c., è apparso legittimo, poiché l'ostensione di tali dati in sede civile è ammessa solo in controversie attinenti alla fatturazione del servizio (nota 31 ottobre 2012).

4.9.1. L'informatica giuridica

Linee-guida per la diffusione dei provvedimenti giudiziari

Le "Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", adottate dal Garante con delibera del 2 dicembre 2010 (in G.U. 4 gennaio 2011, n. 2 [doc. web n. 1774813]), prevedono che l'anonimizzazione del provvedimento giudiziario in caso di riproduzione per finalità di informazione giuridica, mediante oscuramento delle generalità e di ogni altro elemento in grado di identificare l'interessato, può essere disposta dal giudice anche d'ufficio, nei casi in cui la diffusione di informazioni particolarmente delicate possa arrecare conseguenze negative alla vita di relazione o sociale dell'interessato (ad es., in ambito familiare o lavorativo).

Al riguardo sono pervenuti all'attenzione dell'Autorità casi di cittadini che non avevano chiesto l'anonimizzazione della sentenza nel corso del giudizio, come previsto dall'art. 52 del Codice.

Con una segnalazione è stata lamentata la pubblicazione, sul sito internet di un ministero, di una sentenza concernente un procedimento giudiziale in cui era stato coinvolto il segnalante, successivamente indicizzata da un motore di ricerca.

Benché già prima della segnalazione il ministero avesse proceduto, su istanza dell'interessato -presentata oltre i termini di cui all'art. 52 del Codice-, ad anonimizzare la sentenza, la stessa risultava ancora associata al segnalante, digitando il suo nominativo nel motore di ricerca.

Il Garante ha in primo luogo rilevato che l'interessato non aveva presentato all'autorità giudiziaria l'istanza di anonimizzazione della sentenza prima che fosse definito il relativo grado di giudizio, sicché nessuna responsabilità per la pubblicazione integrale del provvedimento poteva attribuirsi al ministero né al motore di ricerca, che si limita ad offrire ospitalità sui propri *server* a siti internet gestiti dai relativi titolari in piena autonomia quale "*mero fornitore del servizio di fruizione della rete … e assolvendo ad un'attività di mero trasporto delle informazioni*" (Cass. civ., sentenza n. 5525/2012; Trib. di Milano, ordinanza 24 marzo 2011).

Il gestore del motore di ricerca, su richiesta dell'Autorità, ha comunque eliminato la copia *cache* relativa alla pagina web oggetto della segnalazione (nota 27 aprile 2012).

In un altro caso l'interessato, lamentando la facile reperibilità in internet di una sentenza penale di condanna emessa nei suoi confronti, completa dei suoi dati identificativi e di informazioni di natura giudiziaria, aveva chiesto di evitare che il proprio nominativo potesse essere utilizzato come chiave di ricerca nei motori presenti in rete, tenuto conto del disagio creato nell'ambito della propria vita personale e professionale dalla facile reperibilità della sentenza.

Il Garante ha sottoposto la vicenda all'attenzione dell'organo giudicante, che accogliendo la richiesta dell'Autorità ha proceduto all'oscuramento della sentenza (nota 18 novembre 2011).

4.9.2. Notificazioni di atti e comunicazioni

Nel 2012 sono pervenute tre sole segnalazioni circa le modalità di notificazione di atti giudiziari in modo non conforme alle prescrizioni del Codice.

Notificazioni di atti giudiziari non a mani proprie

In un caso è stata lamentata la notificazione di un provvedimento giudiziario effettuata dall'ufficio notifiche del tribunale mediante consegna, in assenza dell'interessato, a mani del figlio convivente in plico non sigillato.

Al riguardo il Garante ha ricordato all'ufficio notifiche che l'art. 174 del Codice, nel modificare alcuni articoli dei codici di rito, ha previsto, ove la notifica non possa essere eseguita nelle mani proprie del destinatario, l'inserimento di copia dell'atto in busta chiusa e

sigillata su cui viene apposto il solo numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso.

Il Garante ha quindi richiamato l'ufficio notifiche al rispetto di tali norme, a tutela della riservatezza dei destinatari degli atti (nota 2 aprile 2012).

Notificazioni di atti giudiziari presso il luogo di lavoro

Un cittadino ha lamentato che un agente della Guardia di finanza, al suo rifiuto di ricevere presso il suo luogo di lavoro la notificazione di un provvedimento giudiziario alla presenza dei colleghi dell'interessato, aveva telefonato ai propri superiori per chiedere consigli. Al riguardo l'Autorità non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali, in quanto l'art. 139 c.p.c. prevede espressamente la notificazione di atti giudiziari anche sul luogo di lavoro del destinatario e, nel caso di specie, l'agente si era limitato a chiedere informazioni sulla corretta procedura da seguire, senza divulgare il contenuto dell'atto a terzi (nota 28 agosto 2012).

Con riferimento alla notifica di atti giudiziari mediante fax sul luogo di lavoro, il Garante, nel ricordare anche in questo caso che è ammessa la notificazione di atti sul luogo di lavoro (artt. 138 e 139 c.p.c.) (v. anche provv. 22 ottobre 1998 [doc. web n. 1104097]), ha altresì rilevato che il vigente codice di procedura civile contempla esplicitamente anche l'utilizzo del fax (art. 250 c.p.c., come modificato dall'art. 2, comma 3, d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, con l. 14 maggio 2005, n. 80) (nota 29 febbraio 2012).

5. La sanità

5.1. I trattamenti per fini di cura della salute

Nel 2012 l'Autorità ha continuato ad occuparsi dei trattamenti dei dati sanitari effettuati da soggetti pubblici e privati per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato.

A seguito di alcune segnalazioni, l'Autorità è intervenuta in due casi in cui sia un ambulatorio per la cura di patologie cardiovascolari sia una struttura sanitaria specializzata nella cura di malattie neurologiche avevano inviato a numerosi indirizzi di posta elettronica, visibili a tutti i destinatari, una e-mail riguardante proposte terapeutiche e scelte organizzative degli ambulatori stessi. In tal modo, i destinatari della e-mail erano venuti a conoscenza dei nominativi di tutti gli altri pazienti. A seguito dell'intervento del Garante, le aziende sanitarie hanno curato un adeguato addestramento del personale per evitare il ripetersi di tali incidenti. L'Autorità ha, tuttavia, avviato un procedimento sanzionatorio nei confronti delle aziende sanitarie per la comunicazione a terzi di dati idonei a rivelare lo stato di salute degli interessati senza il loro consenso (note 23 febbraio e 13 novembre 2012).

A seguito di un'altra segnalazione, l'Autorità ha ricordato ad un ospedale lombardo che in caso di accesso da parte del paziente alla cartella clinica, redatta con grafia illeggibile, la stessa deve essere trascritta in modo che le informazioni sanitarie risultino chiare per il malato, essendo la leggibilità la prima condizione per la piena comprensione dei dati personali che riguardano l'interessato (nota 2 febbraio 2012).

L'Autorità è stata chiamata anche ad esprimersi in merito alla possibilità di videoregistrare il parto a cura del marito/convivente.

Al riguardo, il Garante ha ribadito che la videoripresa, da parte di un familiare o di una persona di fiducia, della partoriente che vi si sottoponga volontariamente configura un trattamento di dati per fini esclusivamente personali come tale non soggetto alla disciplina del Codice. Tale esclusione opera esclusivamente nel caso in cui i dati in tal modo raccolti non siano destinati ad una comunicazione sistematica o alla diffusione e siano trattati in ambito familiare o amicale, ferma restando l'autonomia organizzativa della struttura sanitaria

in merito alla facoltà di ammettere i familiari o persone di fiducia del paziente durante lo svolgimento della prestazione sanitaria, nel rispetto di eventuali manifestazioni di volontà contrarie espresse dagli operatori sanitari presenti (nota 2 febbraio 2012).

Nel 2012 l'Autorità è inoltre intervenuta per ricordare al personale medico che deve trattare i dati personali dei pazienti per le sole finalità istituzionali proprie della struttura sanitaria in cui opera e non anche per ulteriori finalità, quali quelle di informare i pazienti circa i recapiti dello studio presso il quale viene svolta attività professionale privata (nota 2 febbraio 2012).

Limiti ancora più stringenti devono ravvisarsi per l'attività di propaganda elettorale a favore di candidati interni alla struttura sanitaria o da questi sostenuti. Il personale medico delle strutture sanitarie non può, infatti, utilizzare per fini elettorali indirizzari o altri dati personali raccolti per fini di cura della salute dell'interessato (nota 13 dicembre 2012).

A seguito di alcune notizie stampa l'Autorità è inoltre intervenuta nei confronti di una società operante in ambito sanitario che dichiarava di essere "*L'unico ente di certificazione riconosciuto (…) dal Garante della privacy per la verifica della conformità dei medical file alle disposizioni contenute nella normativa di settore*". Al riguardo, il Garante ha precisato che attualmente la disciplina in materia di protezione dei dati personali non prevede meccanismi di certificazione, sigilli o marchi di protezione dei dati e spetta solo all'Autorità verificare il rispetto della disciplina in materia di protezione dei dati personali, prescrivendo, se del caso le misure necessarie. L'Autorità ha, pertanto, invitato la società a non lasciar intendere che il suo operato sia autorizzato o riconosciuto dal Garante, nonché a chiedere alla testata giornalistica che aveva riportato la notizia di dare conto di tali precisazioni (nota 21 dicembre 2012).

Tra i diversi casi esaminati merita di essere menzionato uno assai delicato, sotto il profilo della tutela dei dati sensibili, riguardante un sistema di monitoraggio a distanza tramite "etichette intelligenti" (*Rfid*), che in campo sanitario si prestano a molteplici usi, ad esempio per tracciare le sacche di sangue o gli strumenti utilizzati nelle sale operatorie, ovvero per raccogliere dati clinici di pazienti al fine di consentire il controllo a distanza di alcune funzioni vitali (provv. 29 novembre 2012 [doc. web n. 2276103]).

Alcune di queste applicazioni combinano poi l'utilizzo della tecnologia *Rfid* con le tecniche di impianto di *microchip* sottocutaneo su individui.

Il caso trae origine dalla richiesta di una società francese, produttrice di apparecchiature medicali, e di un'azienda ospedaliera volta a valutare la conformità al Codice dei trattamenti di dati effettuati tramite un sistema di monitoraggio remoto di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Il sistema utilizza le etichette intelligenti, inserite nel defibrillatore impiantato sotto la cute del paziente, per consentire agli operatori sanitari di verificare i dati registrati dal dispositivo cardiaco, controllando eventuali anomalie ed effettuando la defibrillazione, ove necessaria, evitando così al paziente la tradizionale visita ospedaliera.

In particolare, le etichette trasmettono i dati registrati dal defibrillatore ad un *monitor* installato a casa del paziente in modalità *wireless*; i dati sono poi trasferiti dal *monitor* al *server* centrale della società attraverso la linea telefonica o *GRPS* per essere consultabili dai medici dell'ospedale via web.

Al riguardo, in considerazione della delicatezza dei dati trattati, è emersa l'esigenza di incrementare il livello di sicurezza delle misure e degli accorgimenti posti in essere, al fine di ridurre i rischi connessi al trattamento dei dati clinici dei pazienti.

L'Autorità ha rilevato -tra l'altro- che la società, per alcune attività di assistenza tecnica, manutenzione e sicurezza del sistema si avvale di operatori esterni in subappalto che possono accedere ai dati clinici dei pazienti. Ha pertanto stabilito che la società designata dall'ospedale responsabile del trattamento può avvalersi per tali attività di terzi subappaltatori -sottoposti ai medesimi obblighi a cui è vincolata la società fornitrice- soltanto previo accordo con l'ospedale. La società deve inoltre inviare all'ospedale i contratti conclusi con i terzi e tenere un elenco aggiornato di tali contratti. Le operazioni di trattamento devono essere registrate e conservate per un periodo di tempo non inferiore a sei mesi. Per evitare che i dati possano essere utilizzati al di fuori del contesto clinico, è stata inoltre prescritta l'adozione di procedure informatiche volte a evitare la copia massiva di dati dal *server* centrale, predisponendo opportuni *alert* in presenza di anomalie.

Qualora i dati registrati dal sistema vengano messi a disposizione di professionisti non

appartenenti alla struttura sanitaria, questi, quali titolari autonomi del trattamento, sono obbligati a raccogliere preventivamente il consenso specifico ed espresso del paziente.

Il paziente inoltre deve poter ottenere in modo agevole la disattivazione del sistema di monitoraggio, con modalità delle quali deve essere data chiara evidenza nel modello di informativa.

L'ospedale deve poi essere tempestivamente informato degli interventi effettuati dal fornitore del servizio o dagli operatori esterni che rendano indispensabile accedere ai dati clinici dei pazienti per esclusive necessità di operatività e di sicurezza del sistema. In particolare, occorre tenere traccia degli utenti abilitati che hanno avuto accesso al servizio e delle altre operazioni eventualmente effettuate anche per consentire all'interessato di controllare i propri dati personali. Tali informazioni devono essere infatti fornite al paziente su sua richiesta.

Le persone autorizzate presso la struttura sanitaria ad accedere al sistema e quelle a vario titolo coinvolte nella manutenzione e nella sicurezza del servizio di monitoraggio devono infine essere adeguatamente istruite sulle funzionalità del sistema e sulle corrette modalità di utilizzo, specie in relazione agli aspetti concernenti la protezione dei dati personali dei pazienti.

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari

Nel 2012 l'Autorità ha ricevuto numerose segnalazioni in merito ai modelli di informativa e di consenso utilizzati in ambito sanitario da parte di strutture pubbliche e private.

In tale ambito il Garante ha prescritto ad una struttura sanitaria privata romana, che aveva fornito prestazioni mediche gratuite nell'ambito di una campagna di prevenzione, di informare correttamente i pazienti sull'uso dei dati, nonché di raccogliere un consenso specifico per ogni tipo di trattamento effettuato (ad es., finalità di cura, comunicazioni a case farmaceutiche), di riformulare i modelli di informativa e consenso per conformarli alla normativa di settore indicando i trattamenti di dati indispensabili all'erogazione della prestazione medica e quelli invece facoltativi (ad es., per finalità di ricerca scientifica, offerta di altri servizi, campagne di prevenzione) ed evidenziando che il mancato consenso per questi ultimi non impedisce di usufruire della prestazione medica richiesta. Il Garante, infine, ha

prescritto alla società di utilizzare i dati finora raccolti esclusivamente per l'esecuzione delle prestazioni sanitarie richieste e per gli adempimenti di legge (es. contabili, fiscali), vietando il loro trattamento per altri tipi di finalità (quali marketing, eventuali comunicazioni a case farmaceutiche) (provv. 9 febbraio 2012 [doc. web n. 1875016]).

Analogamente, ad uno studio radiologico è stato prescritto di modificare i modelli utilizzati per l'informativa ed il consenso, evidenziando per quali dati il conferimento risulti obbligatorio e per quali, invece, facoltativo in relazione alle diverse finalità perseguite, poiché, salvi i casi di emergenza sanitaria, il mancato conferimento dei dati richiesti per le finalità di cura della salute (ivi comprese quelle amministrative a queste strettamente correlate), rende impossibile all'interessato l'accesso alla prestazione sanitaria, mentre il mancato consenso al trattamento dei dati per altre finalità eventualmente perseguite (ad es., ricerca scientifica o invio di referti al medico curante) non deve impedire l'accesso alla prestazione stessa (provv. 15 marzo 2012 [doc. web n. 1893708]).

In termini per vari aspetti simili, è stato fatto presente che qualora il titolare del trattamento intenda effettuare una comunicazione di dati personali a soggetti terzi (ad es., compagnie assicuratrici) non prevista dalla legge, è necessario acquisire uno specifico consenso dell'interessato e specificare nell'informativa se la comunicazione abbia ad oggetto anche dati idonei a rivelare lo stato di salute dell'interessato. In ogni caso, devono essere comunicati a terzi i soli dati indispensabili preferendo, ove possibile, la trasmissione di dati anonimi. A seguito dell'intervento del Garante l'azienda ha provveduto ad inviare un idoneo modello di informativa -attualmente in uso nei rapporti con i pazienti- che risolve le criticità riscontrate dall'Ufficio (nota 13 novembre 2012).

Sono anche state formulate osservazioni sui modelli di informativa e di consenso utilizzati da una azienda ospedaliera torinese con particolare riguardo alla circostanza che il consenso dell'interessato deve essere acquisito dalle aziende sanitarie pubbliche soltanto per il perseguimento delle finalità di cura della salute dell'interessato, e non anche per il trattamento di dati sensibili per finalità di carattere amministrativo, che deve essere conforme alle prescrizioni dello schema tipo di regolamento adottato dalla Conferenza delle regioni e delle province autonome su cui il Garante ha espresso parere favorevole (prov. 26 luglio 2012

[doc. web n. 1915390]; cfr. *infra* par. 5.2.). L'azienda ha conseguentemente modificato i modelli di informativa e consenso (nota 15 novembre 2012).

L'Ufficio è stato chiamato poi a fornire chiarimenti in merito all'obbligatorietà dell'acquisizione del consenso dell'interessato nel caso di trattamenti sanitari iniziati in epoca antecedente alla data di entrata in vigore della normativa in materia di protezione di dati personali. Una struttura sanitaria infatti aveva preso in cura il segnalante nel 1996 avendo poi acquisito il suo consenso al trattamento dei dati sanitari solo nel 2010. Al riguardo, l'Autorità ha ricordato, in base alle norme applicabili (art. 41, comma 1, l. n. 675/1996), che il consenso al trattamento dei dati del segnalante doveva essere acquisito dal primo luglio 2003, sicché il trattamento effettuato sino a quella data deve considerarsi illecito (nota 13 dicembre 2012).

5.1.2. Il fascicolo sanitario elettronico e i dossier sanitari

Già nel 2009 il Garante aveva adottato le "Linee-guida in tema di fascicolo sanitario elettronico (fse) e di *dossier* sanitario"(provv. 16 luglio 2009 [doc. web n. 1634116]) per rispondere, da un lato, alla mancanza a livello nazionale di una normativa quadro, dall'altro, al monito rivolto in sede europea dal Gruppo Art. 29 sulla necessità di individuare specifiche cautele per il trattamento dei dati personali nell'ambito di progetti di sanità elettronica.

Recentemente, con il d.l. 18 ottobre 2012, n. 179 ("Ulteriori misure urgenti per la crescita del Paese") convertito dalla l. 17 dicembre 2012, n. 221, è stata fornita una definizione di fascicolo sanitario elettronico corrispondente a quella elaborata dall'Autorità, individuando quale presupposto legittimante per il suo utilizzo il consenso dell'interessato, così come indicato dal Garante nelle predette linee-guida.

La citata normativa prevede che con decreto del Ministro della salute e del Ministro delegato per l'innovazione tecnologica, acquisito il parere del Garante, dovranno essere stabiliti -tra l'altro- i contenuti del fse, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al fse. Nel gennaio del 2013 l'Autorità è stata invitata a partecipare al tavolo di lavoro istituito presso il Ministero della salute per l'elaborazione di tale schema di decreto.

Nel 2012, da un accertamento ispettivo, è emerso che le strutture sanitarie pubbliche del Friuli Venezia Giulia utilizzavano un *dossier* sanitario strutturato in modo tale da consentire a tutti i medici -inserendo *username* e *password*- di accedere ai referti di qualsiasi persona avesse effettuato in passato un esame clinico presso le diverse strutture sanitarie della Regione, indipendentemente dalla circostanza che il paziente fosse in cura presso il medico che effettuava il suddetto accesso.

Il Garante, rilevata l'illiceità del trattamento in ragione anche della mancanza di informativa e consenso, ha prescritto, in particolare, che i documenti sanitari attualmente utilizzati attraverso il *dossier* sanitario restino disponibili solo al professionista o alla struttura interna al titolare che li ha redatti (es. informazioni relative a un ricovero utilizzabili dal reparto di degenza) nonché per eventuali conservazioni per obbligo di legge, con l'adozione di idonei accorgimenti anche tecnici, affinché i medesimi documenti sanitari non siano più condivisi con altri professionisti che curino l'interessato presso altri reparti, fino al momento in cui lo stesso esprima uno specifico consenso.

Il Garante ha, inoltre, prescritto a tali strutture sanitarie di mettere in atto, entro un breve periodo, specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in quel momento in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del *dossier*) di accedere al suo *dossier* sanitario per il tempo in cui si articola il percorso di cura (provv. 10 gennaio 2013 [doc. web n. 2284708]).

5.1.3. I referti

L'Autorità è stata chiamata più volte ad intervenire in merito alla possibilità di comunicare le informazioni relative allo stato di salute degli assistiti, ai loro parenti e familiari senza aver acquisito prima uno specifico consenso.

In tali occasioni il Garante ha ribadito che per comunicare dati sensibili per fini di cura a soggetti diversi dall'interessato, in assenza di una disposizione normativa, si dovrà richiedere uno specifico consenso informato a quest'ultimo. Nel caso in cui l'interessato stesso sia incapace di intendere o volere, il consenso deve essere manifestato da parte del legale rappresentante (nota 11 dicembre 2012).

Da notizie stampa l'Ufficio ha appreso la vicenda che in un ospedale in provincia di Milano ad un paziente era stato consegnato al posto del suo referto quello di un altro paziente. Il Garante, sulla base dei riscontri richiesti all'ospedale, ha evidenziato l'illiceità della consegna del referto avviando un procedimento sanzionatorio e prescrivendo all'ospedale di fornire agli incaricati del trattamento dati apposite istruzioni affinché la consegna dei referti avvenga previa verifica dell'identità dell'interessato, o del soggetto da questo delegato, con consegna a quest'ultimo in busta chiusa (provv. 1° marzo 2012 [doc. web n. 1893694]). L'esigenza che informazioni sullo stato di salute siano consegnate a terzi incaricati sulla base di delega scritta, mediante busta chiusa, è stata ribadita anche successivamente. Tale misura non occorre invece nella consegna diretta all'interessato (note 15 novembre e 19 dicembre 2012).

In un altro caso, una paziente di una azienda sanitaria del nord Italia lamentava l'avvenuto invio del referto relativo all'esame istologico dei campioni di tessuto abortivo ad essa prelevati all'indirizzo di residenza del padre. Dalla documentazione agli atti è emerso che la paziente non aveva mai fornito tale indirizzo come recapito presso il quale ricevere comunicazioni da parte dell'azienda sanitaria. Nei confronti di questa è stato pertanto avviato un procedimento sanzionatorio per trattamento illecito di dati personali (nota 27 aprile 2012).

L'esigenza che le informazioni sullo stato di salute siano comunicate all'interessato solo per il tramite di un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente e che gli esiti di esami clinici effettuati siano accompagnati dall'indicazione della disponibilità del medico a fornire ulteriori indicazioni a richiesta è stata richiamata con nota del 6 settembre 2012 .

In relazione alla notizia apparsa su alcuni organi di stampa relativa all'avvenuta installazione presso un'azienda sanitaria toscana di un "totem" a disposizione dei pazienti per la stampa dei referti, il Garante ha ricordato in particolare che devono essere adottate soluzioni, quali la previsione di distanze di cortesia, tali da prevenire l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dell'interessato (nota 11 maggio 2012).

5.1.4. La tutela della dignità della persona

Anche nel 2012 l'Autorità è stata chiamata più volte ad intervenire sulla violazione delle misure previste dal Codice a tutela della dignità delle persone in ambito sanitario (art. 83).

In particolare, ad una azienda sanitaria che apponeva sull'esterno delle buste contenenti la corrispondenza diretta ai pazienti un timbro recante la dicitura "Dipartimento di salute mentale" è stato ricordato che non devono essere indicate sulla parte esterna del plico postale spedito al domicilio dell'interessato, informazioni idonee ad essere correlate con lo stato di salute dell'interessato stesso. A seguito dell'intervento del Garante la struttura sanitaria ha tolto con immediatezza la dicitura posta all'esterno delle buste (nota 28 giugno 2012).

Analogamente l'Ufficio, a seguito di una segnalazione, è intervenuto per evitare che una struttura sanitaria della Regione Campania indicasse sulle certificazioni, richieste dal paziente per la giustificazione di un assenza dal lavoro, il dipartimento ove si era recato il paziente stesso. A seguito dell'intervento del Garante la struttura sanitaria ha distribuito ai reparti un idoneo modello di certificazione (nota 9 gennaio 2012).

Una lamentela costante nel corso degli anni, oggetto ancora di numerose segnalazioni, riguarda la mancata adozione, da parte di strutture sanitarie, di soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute. A seguito degli interventi dell'Ufficio, le strutture sanitarie interpellate hanno provveduto a introdurre le distanze di cortesia nelle prossimità degli sportelli per l'accettazione dei pazienti, nonché altre soluzioni tecniche per evitare la conoscibilità di dati sensibili degli interessati da parte di terzi estranei (note 18 gennaio, 9 luglio, 9 agosto e 6 settembre 2012).

5.1.5. Il trattamento di dati personali in occasione dell'accertamento dell'infezione da HIV

Nel 2012 il Garante è più volte intervenuto in merito alle garanzie da adottare nel trattamento dei dati personali di pazienti affetti da HIV.

In particolare, poiché da una segnalazione risultava che in un pronto soccorso milanese non erano state adottate misure tali da evitare che le informazioni relative allo stato di sieropositività del segnalante fossero conosciute da terzi, il Garante ha ricordato gli specifici

obblighi previsti dalla legge, in base ai quali l'operatore sanitario che viene a conoscenza di un caso di infezione da HIV è tenuto a prestare la necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità (art. 5, l. n. 135/1990, così come modificato dall'art. 178 del Codice) (nota 18 ottobre 2012).

Altra segnalazione riguardava la possibilità di consegnare i risultati degli accertamenti diagnostici in materia di HIV a persona munita di idonea delega dell'interessato. Al riguardo, il Garante ha ricordato che le specifiche disposizioni in base alle quali gli operatori sanitari devono comunicare i risultati degli accertamenti diagnostici, diretti o indiretti per l'infezione da HIV, "*esclusivamente alla persona cui tali esami sono riferiti*" (art. 5, commi 1 e 4, l. n. 135/1990) (v. Relazione 2008 p. 92), rappresentano un limite speciale più restrittivo, in materia di trattamento dei dati relativi all'infezione da HIV, rispetto alla regola generale, che ammette la consegna in busta chiusa al terzo a tal fine delegato (nota 3 ottobre 2012).

5.1.6. La ricerca scientifica

Si è riferito nella Relazione 2011 (cfr. p. 77) dell'autorizzazione generale al trattamento dei dati personali effettuati per eseguire studi e ricerche in campo medico, biomedico e epidemiologico nel caso in cui risulti impossibile rendere l'informativa agli interessati con scadenza il 31.12.2012 (provv. 1° marzo 2012, in G.U. 26 marzo 2012, n. 72 [doc. web n. 1878276]).

Nel 2012, l'Ufficio ha in diverse occasioni comunicato a enti di ricerca, organismi sanitari, società scientifiche ed università richiedenti che, sulla base di tale autorizzazione, non è più necessario ottenere, caso per caso, specifiche autorizzazioni da parte dell'Autorità.

L'Ufficio ha inoltre sottolineato che non è consentito avvalersi della deroga all'obbligo di raccogliere il consenso degli interessati nei casi in cui sia effettivamente possibile fornire loro un'adeguata informativa. La possibilità di trattare dati sulla salute anche a prescindere dal consenso è infatti ammessa in via residuale dall'art. 110 del Codice in presenza di particolari e comprovate circostanze dalle quali derivi l'impossibilità di informare gli interessati, purché lo studio abbia ottenuto dal comitato etico motivato parere favorevole.

Lo ha precisato l'Ufficio, in un caso riguardante una società farmaceutica che intendeva svolgere uno studio clinico non interventistico multinazionale, in assenza del consenso degli interessati, senza però evidenziare situazioni eccezionali o particolari che rendevano impossibile informare i pazienti coinvolti. Il protocollo dello studio prevedeva peraltro che sarebbe stato ugualmente possibile realizzare gli obiettivi dello studio stesso anche se, in base alle norme applicabili, fosse stato necessario acquisire il consenso degli interessati (nota 17 dicembre 2012).

Alla fine del 2012, l'autorizzazione è stata rinnovata per un anno, insieme alle altre autorizzazioni generali, senza significative modifiche, fatta eccezione per i tipi di dati oggetto di trattamento (autorizzazione generale n. 9/2012 al trattamento dei dati personali effettuato per scopi di ricerca scientifica, provv. 13 dicembre 2012, pubblicato in G.U. 4 gennaio 2013, n. 3 [doc. web n. 2159932]). In linea con le modifiche apportate alla autorizzazione generale n. 2, sono state ampliate le categorie di dati sensibili che possono essere trattate, poiché un elevato numero di trattamenti nel settore sanitario è effettuato anche con informazioni sulla vita sessuale e origine razziale ed etnica degli interessati (v. punto 1.2. autorizzazione generale n. 2/2012 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - provv. 13 dicembre 2012, in G.U. 4 gennaio 2013, n. 3 [doc. web n. 2158850]).

Ove necessario per la ricerca, la detta autorizzazione n. 9/2012, efficace sino al 31 dicembre 2013, consente pertanto non solo l'utilizzo di dati sulla salute, ma anche sulla vita sessuale e sull'origine razziale ed etnica, in assenza del consenso dei pazienti interessati, qualora non sia possibile informarli sul trattamento dei loro dati per "motivi etici" o "motivi di impossibilità organizzativa" e a condizione che sul progetto di ricerca si sia espresso favorevolmente, con parere motivato, il comitato etico territorialmente competente (artt. 107 e 110 del Codice). Rimane invece confermato l'obbligo di acquisire il consenso dei pazienti nei casi in cui risultino reperibili e, in particolare, quando si rivolgano nuovamente al centro di cura, anche per visite di controllo.

È invece necessaria una specifica autorizzazione del Garante per circostanze del tutto particolari o situazioni eccezionali non considerate nell'autorizzazione generale.

È stato questo il caso di una società farmaceutica statunitense che ha richiesto di essere autorizzata ad utilizzare dati attinenti alla salute e all'origine razziale ed etnica di pazienti adulti gravi con gravi lesioni traumatiche e *shock* emorragico per effettuare una sperimentazione clinica multinazionale volta a valutare l'efficacia della terapia con un farmaco sperimentale in aggiunta alle cure ordinarie.

Secondo quanto rappresentato dalla società, le gravi condizioni cliniche dei pazienti coinvolti avrebbero potuto determinare uno stato di incoscienza e avrebbero reso necessari interventi di soccorso immediato come la ventilazione artificiale o una terapia analgesica oppioide; tali circostanze avrebbero reso impossibile, al momento dell'arruolamento nello studio, rendere l'informativa a tutti i pazienti interessati ed ottenerne il consenso.

Al riguardo il Garante ha ritenuto che le particolari garanzie previste dal Codice per i trattamenti di dati a fini di cura, nei casi in cui manchi il consenso dell'interessato, incapace o altrimenti impossibilitato a prestarlo (art. 82, comma 2), debbano operare anche nel caso sottoposto dalla società, invitata pertanto a privilegiare il consenso delle persone più vicine al paziente, che sono in condizione di salvaguardarne meglio la volontà. Solo in assenza di queste, in condizioni di emergenza, può essere coinvolto il medico responsabile dell'ospedale, fermo restando che questo consenso può essere revocato dai familiari qualora si rendessero disponibili successivamente.

Essendo molto ridotto il numero delle persone incluse nello studio presso l'unico centro di sperimentazione situato in Italia, il Garante ha poi prescritto alla società farmaceutica e al centro di assegnare a ciascuna persona un codice alfanumerico casuale che non contenga le iniziali del nome e cognome, in modo da ridurre il rischio di re-identificazione degli interessati.

La società è stata quindi autorizzata ad effettuare il trattamento tenendo anche in considerazione che i dati saranno utilizzati solo per finalità statistiche e di ricerca medica e potranno essere comunicati ad altre società esterne che collaborano alla sperimentazione, situate in Paesi terzi solo in forma codificata e nel rispetto delle garanzie previste dal Codice per il trasferimento dei dati all'estero. Le informazioni inoltre saranno conservate presso il centro di sperimentazione per un massimo di sette anni. Per proteggere i dati dei pazienti

dovranno essere poi adottate specifiche misure di sicurezza e adeguati accorgimenti tecnici. Resta infine fermo l'obbligo di raccogliere direttamente il consenso informato dei pazienti qualora questi siano in condizioni di fornirlo (provv. 25 ottobre 2012 [doc. web n. 2120934]).

Sempre con riferimento alle sperimentazioni cliniche sui farmaci, nel rispondere ad alcuni quesiti posti da una società farmaceutica, l'Ufficio ha fornito indicazioni sulla videoregistrazione delle interviste a pazienti affetti da schizofrenia, condotte da medici sperimentatori nell'ambito di uno studio clinico, allo scopo di verificare in modo più efficace l'accuratezza dell'intervista e il rispetto da parte dello sperimentatore delle procedure previste dal protocollo di studio.

Alla luce dei princìpi di proporzionalità e finalità, l'utilizzo del sistema di videoregistrazione può ritenersi giustificato soltanto se, nel caso concreto, non si possa ricorrere a sistemi di controllo meno invasivi della sfera di autodeterminazione di medici e pazienti interessati (v. artt. 3 e 11 del Codice).

In secondo luogo, il preventivo consenso dei medici e pazienti coinvolti deve essere "validamente prestato" (artt. 23 e 107 del Codice e punto 1.2., lett. *a)*, autorizzazione n. 2 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale), ossia gli interessati devono essere realmente in grado di operare una scelta senza alcuna forma di coercizione, come potrebbe invece accadere in caso di persone incapaci d'intendere e di volere o nel contesto di un rapporto di lavoro (cfr. al riguardo, Gruppo Art. 29, parere del 13 luglio 2011, n. 15 sulla definizione di consenso). In tale ambito, è poi necessario assicurare il rispetto della disciplina sul controllo a distanza dei lavoratori, in ipotesi configurabile nei confronti di medici dipendenti delle strutture ospedaliere presso cui viene svolta la sperimentazione (v. art. 4 l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice).

In terzo luogo, per quanto riguarda le modalità del trattamento, occorre verificare, in particolare, se gli obiettivi del trattamento possano essere utilmente realizzati senza che i pazienti ripresi siano riconoscibili, ovvero evitando di raccogliere dati, anche sulla salute, non indispensabili per le finalità cui la videoregistrazione è preordinata (art. 11 del Codice e punto 3., autorizzazione n. 2/2011 cit.).

Infine, è stata sottolineata l'esigenza di adottare le misure individuate nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 [doc. web n. 1712680], specie per quanto riguarda l'informativa agli interessati, i responsabili del trattamento e le misure di sicurezza, nonché il trasferimento dei dati all'estero (artt. 13, 29, 33-35 e 44 del Codice).

5.2. I TRATTAMENTI PER FINI AMMINISTRATIVI

L'Autorità ha più volte fornito indicazioni in merito ai trattamenti di dati sensibili e, in particolare, di quelli idonei a rivelare lo stato di salute, effettuati da strutture sanitarie pubbliche per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal servizio sanitario nazionale (art. 85, comma 1, lett. *a*), del Codice).

Al riguardo, l'Ufficio ha ricordato alle strutture sanitarie pubbliche che quando perseguono finalità amministrative correlate alle finalità di cura non devono acquisire il consenso dell'interessato (note 13 e 15 novembre 2012).

Inoltre, nel 2012 il Garante ha espresso parere favorevole sullo schema tipo aggiornato di regolamento predisposto dalla Conferenza delle regioni e delle province autonome. Il nuovo testo finalizzato a garantire un più ampio quadro di tutele rispetto ai flussi crescenti di dati scambiati tra le pubbliche amministrazioni, anche in ragione delle nuove competenze e dell'esigenza di verificare il buon andamento dell'attività amministrativa, è frutto di un complesso e proficuo lavoro di collaborazione del Garante con la Conferenza delle regioni e delle province autonome, che ha visto presenti tutte le amministrazioni interessate.

Nell'esprimere il parere, l'Autorità ha chiesto che lo schema venga integrato con specifiche garanzie: ad esempio, che ai fini del monitoraggio e valutazione dell'efficacia dei trattamenti sanitari erogati, le regioni, una volta acquisiti i dati dalle Asl, adottino un sistema di codifica che non consenta l'identificazione diretta del soggetto interessato. Inoltre, ha ritenuto che non fosse indispensabile l'utilizzo di dati sensibili, quale l'adesione a partiti, sindacati, associazioni religiose, per finalità di programmazione, gestione e valutazione dell'assistenza sanitaria (provv. 26 luglio 2012 [doc. web n. 1915390]).

Le regioni e le province autonome che intendono aggiornare, sulla base del nuovo schema tipo, i propri atti regolamentari sul trattamento dei dati sensibili e giudiziari, dovranno

pertanto recepire le indicazioni formulate dal Garante nel predetto parere. Gli atti regolamentari adottati sulla base dello schema tipo modificato in conformità alle indicazioni ivi contenute, non dovranno invece essere sottoposti nuovamente al Garante.

Nel parere, l'Autorità ha anche espresso le sue valutazioni in ordine al decreto del Ministero della salute concernente il sistema di sorveglianza delle nuove diagnosi di infezioni da HIV, richiamato dallo schema tipo e che risultava essere stato emanato senza il previsto parere del Garante (art. 154, comma 4 del Codice).

A questo proposito, dopo aver rappresentato, tra l'altro, che la mancata consultazione vizia gli atti adottati per violazione di legge, sono state evidenziate talune criticità. È stato sottolineato, in particolare, che il codice identificativo, individuato dal decreto per la notifica dei nuovi casi di infezione da HIV, non è idoneo a garantire la non identificazione della persona interessata come invece previsto dalla l. 5 giugno 1990, n. 135 (art. 5); inoltre le modalità di trasmissione delle notifiche previste dal decreto non garantiscono un adeguato livello di sicurezza rispetto alla natura dei dati oggetto di trattamento nei confronti dei quali l'ordinamento richiede cautele più rigorose (artt. 31 e 178, comma 2, del Codice).

Al riguardo, è stato dato atto che il Ministero della salute ha espresso l'intenzione di avviare un percorso collaborativo con l'Autorità ai fini dell'acquisizione del previsto parere. In tale quadro, pertanto, i trattamenti di dati sensibili possono essere effettuati dalle aziende sanitarie, dalle regioni e dalle province autonome, nell'ambito delle attività amministrative correlate alla sorveglianza epidemiologica dei casi di infezione da HIV, nel rispetto delle specifiche cautele che saranno individuate dal Ministero della salute, in collaborazione con l'Autorità.

Per quanto riguarda l'attivazione dei nuovi flussi di dati tra i medici prescrittori e il Ministero dell'economia e delle finanze, a fini di monitoraggio della spesa sanitaria e verifica dell'appropriatezza prescrittiva, (introdotti dal comma 5-*bis*, art. 50 d.l. 30 settembre 2003, n. 269 convertito dalla l. 24 novembre 2003, n. 326), il Garante ha rilevato che è necessario modificare il protocollo, sottoscritto in data 9 marzo 2006 sentita l'Autorità, con cui sono individuati i dati in possesso del Mef che possono essere trasmessi al Ministero della salute e alle regioni e le modalità di tale trasmissione (comma 10, dell'art. 50 cit.).

In argomento il Garante, su richiesta del Mef, si è dichiarato disponibile ad avviare, insieme con le amministrazioni sottoscrittrici del protocollo, un'attività collaborativa per estendere le cautele già previste per i flussi relativi ai dati contenuti nelle prescrizioni di farmaci e di prestazioni specialistiche anche ai nuovi flussi originati dai medici prescrittori.

In considerazione delle specifiche competenze attribuitele dal legislatore in alcune materie, la Provincia autonoma di Trento ha chiesto un parere al Garante sulle modifiche e integrazioni da apportare ad alcune schede dello schema tipo aggiornato di regolamento per il trattamento di dati sensibili e giudiziari presso le regioni e le province autonome, le aziende sanitarie, gli enti e agenzie regionali/provinciali, nonché gli enti vigilati, già valutato positivamente dall'Autorità il 26 luglio 2012 [doc. web n. 1915390]. Tali modifiche e integrazioni sono riferibili ai trattamenti di dati personali effettuati in materia di interventi assistenziali in favore degli invalidi civili, dei ciechi civili e dei sordomuti, nonché alla gestione dei procedimenti per l'interdizione anticipata dal lavoro delle lavoratrici in gravidanza.

Il Garante ha espresso parere favorevole sulla versione aggiornata delle predette schede proposta dalla Provincia, che ha tenuto conto delle osservazioni formulate, in via collaborativa, dall'Ufficio (parere 8 novembre 2012 [doc. web n. 2216879]).

Più in dettaglio, con riferimento alle suddette competenze in materia di interdizione della lavoratrice in gravidanza trasferite alle aziende sanitarie locali, l'Autorità ha stabilito che le regioni e province autonome, nell'adeguare il proprio regolamento per il trattamento dei dati sensibili e giudiziari allo schema tipo aggiornato (oggetto del citato parere favorevole del Garante del 26 luglio 2012 [doc. web n. 1915390] facciano riferimento alle modifiche e integrazioni apportate dalla Provincia autonoma di Trento alla rispettiva scheda allegata, senza dover richiedere all'Autorità uno specifico parere. A tal fine sono stati individuati in un documento allegato al parere i tipi di dati trattati e le operazioni eseguibili dalle aziende sanitarie locali in relazione alle finalità di rilevante interesse pubblico di cui all'art. 86, comma 1, lett. *a)*, del Codice.

L'Ufficio ha inoltre fornito chiarimenti ad un medico accreditato con il Servizio sanitario nazionale in merito alla legittimità della richiesta, avanzata da un funzionario del distretto

sanitario nell'esercizio delle proprie funzioni di controllo sulle prestazioni erogate, di esibire i referti relativi a determinate visite.

In proposito l'Ufficio ha ricordato che nella scheda n. 9 (Assistenza sanitaria di base: assistenza sanitaria in forma indiretta) del citato schema tipo di regolamento è previsto che i dati possono essere comunicati ai soggetti/strutture aziendali che erogano prestazioni (medico del distretto, medico ospedaliero) per la gestione amministrativa ed economica; che l'azienda sanitaria ha l'esigenza di svolgere attività di monitoraggio, controllo e valutazione dell'efficacia dei trattamenti sanitari erogati (artt. 8-*octies* e 10 d.lgs. n. 502/92). In particolare, il trattamento dei dati ha l'obiettivo di caratterizzare l'esposizione a fattori di rischio, ricostruire i percorsi assistenziali e identificare/confrontare gli esiti di salute, valutare e confrontare (tra gruppi di popolazione o tra strutture) l'appropriatezza, l'efficacia e l'efficienza dell'assistenza erogata; per tali scopi l'azienda sanitaria ha necessità di effettuare la selezione, l'estrazione, la conservazione, il raffronto, l'interconnessione e l'elaborazione (con modalità informatizzate) dei diversi archivi di dati personali correnti gestiti nell'ambito del sistema informativo sanitario aziendale (nota 13 novembre 2012).

L'Ufficio ha anche fornito chiarimenti ad una azienda sanitaria toscana circa la possibilità di comunicare alla protezione civile i dati dei propri assistiti ai fini della predisposizione dei piani di protezione civile. In merito, ha ricordato che nella scheda n. 6 (Attività di assistenza socio-sanitaria a favore di fasce deboli di popolazione e di soggetti in regime di detenzione) del citato schema tipo di regolamento è previsto che le aziende sanitarie comunichino "*ove necessario, alle strutture che svolgono compiti di protezione civile (regione, agenzie regionali, comuni) i dati sanitari delle persone interessate dagli interventi di protezione civile, per poter predisporre tali interventi nell'ambito dei piani di emergenza (l. n. 225/1992 e l. n. 353/2000*)". Con specifico riferimento ai dati dei pazienti che utilizzano apparecchiature elettromedicali indispensabili alla vita, la medesima scheda prevede inoltre che le aziende sanitarie comunichino "*all'Enel o ad altro soggetto gestore dell'energia elettrica l'elenco dei soggetti con apparecchiature elettromedicali indispensabili alla vita al fine di assicurare loro la continuità di fornitura di energia elettrica nei casi di interruzione programmata e/o eccezionale della corrente*". In tal quadro, pertanto, l'azienda sanitaria, sulla base di quanto indicato dall'amministrazione richiedente, dovrà

valutare autonomamente la tipologia di assistiti, ivi comprese le persone che utilizzano apparecchiature elettromedicali indispensabili alla vita, che possono essere interessati dai suddetti interventi di protezione civile e conseguentemente comunicare alle strutture che svolgono compiti di protezione civile i soli dati sanitari che riterrà indispensabili al fine di consentire la realizzazione dei previsti interventi (nota 21 dicembre 2012).

Nel corso dell'anno l'Ufficio ha avviato un'attività di controllo sui trattamenti di dati connessi alla tenuta dei registri di monitoraggio dei farmaci istituiti dall'Agenzia italiana del farmaco (Aifa), per controllare la spesa sanitaria in relazione alla correttezza delle prescrizioni dei farmaci erogabili a totale carico del Ssn.

Questi farmaci sono rimborsabili nel rispetto di specifiche condizioni poste dall'Aifa in relazione a ciascun medicinale e sulla base di quanto stabilito dagli accordi negoziati con le società farmaceutiche produttrici. Per verificare la correttezza delle procedure ammnistrative volte a ottenere l'eventuale rimborso, l'Aifa richiede ai centri utilizzatori dei medicinali di raccogliere su schede in formato elettronico dati relativi alle condizioni di salute dei pazienti eleggibili e dati di *follow-up* periodico e di memorizzarli nei predetti registri tramite un'applicazione web accessibile dal sito istituzionale dell'Agenzia.

Tra i medicinali sottoposti a monitoraggio vi sono poi quelli innovativi, sottoposti a sperimentazione clinica e non ancora autorizzati all'immissione in commercio e i medicinali impiegati per indicazioni terapeutiche diverse da quelle autorizzate. Tali farmaci, inseriti nell'elenco di cui alla l. n. 648/1996 predisposto dall'Aifa, sono sottoposti anche ad un monitoraggio clinico che implica la trasmissione all'Agenzia di dati clinici raccolti dalle strutture prescrittrici per verificarne l'appropriatezza d'uso. Inoltre, se il farmaco è inserito nell'elenco dei medicinali sottoposti a monitoraggio intensivo di farmacovigilanza di cui al d.m. 21 novembre 2003 è prevista altresì la raccolta di dati relativi a sospette reazioni avverse.

In tale quadro, gli approfondimenti curati dall'Ufficio sono volti a verificare, in particolare, l'idoneità dei presupposti giuridici che legittimerebbero il trattamento dei dati destinati a confluire nei registri di monitoraggio dei farmaci istituiti dall'Aifa, il rispetto dell'obbligo dell'informativa agli interessati, la pertinenza, non eccedenza e l'indispensabilità dei dati trattati per la tenuta dei registri, l'ambito di comunicazione e di diffusione dei dati

memorizzati nei registri, nonché gli accorgimenti posti in essere per tutelare l'identità e la riservatezza dei pazienti e le misure di sicurezza adottate.

Come più diffusamente esposto nel paragrafo 3.3.1. della presente Relazione, nel 2012 il Garante ha inoltre espresso il proprio parere favorevole su tre schemi di decreto del Ministero della salute volti ad istituire nell'ambito del nuovo sistema informativo sanitario ulteriori flussi telematici di dati finalizzati a consentire il monitoraggio della spesa sanitaria. Tali decreti riguardano, in particolare, le prestazioni di emergenza-urgenza erogate sia dal 118, sia dai presidi ospedalieri di pronto soccorso (parere 21 marzo 2012 [doc. web n. 1892560]), le prestazioni residenziali e semiresidenziali per anziani o persone non autosufficienti (parere 17 aprile 2012 [doc. web n. 1907937]), le prestazioni farmaceutiche effettuate in distribuzione diretta o per conto delle asl (parere 11 maggio 2012 [doc. web n. 1900890]), nonché il sistema informativo di monitoraggio dell'assistenza domiciliare (parere 29 marzo 2012 [doc. web n. 1893476]).

In particolare nel rendere il proprio parere sui predetti schemi, il Garante ha richiesto di precisare le finalità cui è preordinato il monitoraggio, di eliminare i riferimenti alla raccolta di informazioni suscettibili di identificare, anche indirettamente l'interessato (ad es., la data o il mese di nascita, il numero del ricovero), di rispettare il principio di proporzionalità nel trattamento dei dati, con particolare riguardo alle informazioni relative alle patologie da cui è affetto l'interessato o attinenti la sfera più intima della persona (ad es., informazioni riguardanti le violenze sessuali subite), e di utilizzare tecniche di cifratura al fine di proteggere le predette informazioni; ha altresì indicato i parametri ai quali devono conformarsi le trasmissioni telematiche dei dati al sistema.

6. I DATI GENETICI

Il Garante ha rinnovato per tutto il 2013 l'autorizzazione generale in materia (provv. 13 dicembre 2012, in G.U. 4 gennaio 2013, n. 3 [doc. web n. 2157564]).

La nuova autorizzazione è sostanzialmente analoga alla precedente (cfr. Relazione 2011 p. 79), poiché è risultata uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati ed ha reso superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento.

L'autorizzazione afferma in particolare il diritto dell'interessato di scegliere se essere informato o meno dei risultati degli esami genetici, comprese eventuali notizie inattese che lo riguardano, qualora queste ultime rappresentino un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive (punti 5 e 6 autorizzazione cit.).

Al riguardo, nel rispondere alla richiesta di chiarimenti pervenuta da un comitato etico di un'azienda ospedaliera universitaria, l'Ufficio ha precisato che il diritto dell'interessato di scegliere se essere informato deve essere garantito anche quando, al momento iniziale della raccolta dei dati nell'ambito di uno studio scientifico, seppure non sia possibile definire nel dettaglio quali geni saranno analizzati, non è escluso che in futuro i risultati ottenuti possano essere rilevanti per la salute dell'interessato stesso, specie nel caso in cui lo studio preveda il sequenziamento dell'intero genoma. A tal fine, possono essere approntati opportuni meccanismi di comunicazione e di informazione che consentano agli interessati di scegliere di volta in volta se essere o non essere messi a conoscenza dei risultati ottenuti nel corso della ricerca (nota 14 gennaio 2013).

7. La statistica

7.1. Censimenti

7.1.1. 15° Censimento generale della popolazione e delle abitazioni

Nell'ottobre del 2011 si è svolto il 15° Censimento generale della popolazione e delle abitazioni. L'Autorità è stata chiamata a garantire che nella sua realizzazione fosse prestata adeguata tutela ai diritti degli interessati in relazione al trattamento dei loro dati personali.

Il Censimento, indetto in esecuzione del Regolamento comunitario n. 763/2008 e dell'art. 50 del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122, è stato inserito, con la redazione dell'apposito prospetto identificativo, nel Programma statistico nazionale 2011-2013 sul quale il Garante si è espresso con parere del 23 settembre 2010 [doc. web n. 1753181].

La complessa materia ha evidenziato una serie di profili problematici, di seguito sintetizzati.

Parere sul Piano generale di censimento

L'Istat ha organizzato le operazioni relative al Censimento attraverso un Piano generale di censimento, sottoposto all'Autorità in particolare per le sezioni relative all'obbligo di risposta, alle sanzioni, al trattamento dei dati, alla diffusione e alla comunicazione.

Dall'analisi dei questionari è risultato come, oltre alle informazioni idonee a rivelare lo stato di salute fornite volontariamente dagli interessati sulla base di quanto correttamente indicato nel Psn 2011-2013, l'Istituto avesse inteso acquisire anche informazioni idonee a rivelare la vita sessuale degli interessati, richiedendo di indicare la relazione di parentela o di convivenza con l'intestatario del foglio famiglia, specificando anche la condizione di convivente "*in coppia di sesso diverso*" o "*in coppia dello stesso sesso*". Pertanto, l'Autorità, nell'esprimere parere favorevole sul piano generale di censimento, ha osservato che l'Istat, per rilevare correttamente anche tali informazioni, avrebbe dovuto indicarle in un atto di natura regolamentare ovvero integrare il Psn 2011-2013, specificando anche nei questionari di censimento che non vi è al riguardo obbligo di risposta da parte dell'interessato. Il Garante ha, inoltre, ritenuto opportuno che gli interessati fossero adeguatamente informati anche sulla circostanza che i dati anagrafici contenuti nella lista dei questionari di famiglia e convivenza sarebbero stati

trattati da parte dei comuni per la revisione post-censuaria delle anagrafi, oltreché dall'Istat per finalità statistiche (art. 50, d.l. 78/2010, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122) (parere 16 febbraio 2011 [doc. web n. 1797064]).

Successivamente l'Istituto ha comunicato all'Autorità di voler utilizzare la dicitura "*convivente in coppia dell'intestatario*", riferibile sia a coppie dello stesso sesso sia a coppie di sesso differente, ed il Garante ha preso atto di tale scelta (provv. 23 marzo 2011 [doc. web n. 1801731]).

Attività di controllo

Sulla base di alcune segnalazioni e notizie stampa, il Garante ha avviato alcune specifiche istruttorie volte a verificare, anche in collaborazione con l'Istat, il rispetto della normativa in materia di dati personali nell'ambito dell'esecuzione del 15° Censimento generale della popolazione e delle abitazioni.

In particolare, oggetto di controllo sono state le attività svolte da alcuni uffici comunali nell'ambito della raccolta e della tenuta dei questionari censuari. All'esito delle istruttorie, svoltesi anche attraverso accertamenti ispettivi *in loco* da parte dell'Istituto, è emersa la correttezza del trattamento dei dati (nota 28 maggio 2012).

7.1.2. 9° Censimento generale dell'industria e dei servizi e Censimento delle istituzioni non profit

Nel 2012, l'Istat ha organizzato le operazioni relative al 9° Censimento generale dell'industria e dei servizi e Censimento delle istituzioni *non profit* attraverso la predisposizione del relativo "Piano generale di Censimento" (art. 50, comma 2, d.l. 31 maggio 2010, n. 78 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 30 luglio 2010, n. 212). Nel piano sono stati individuati, in particolare, i soggetti tenuti all'obbligo di risposta, le modalità di diffusione dei dati anche con frequenza inferiore alle tre unità -ad esclusione dei dati di cui all'art. 22 del Codice-, la comunicazione dei dati elementari ai soggetti facenti parte del Sistema statistico nazionale, nonché la comunicazione agli organismi di censimento dei dati elementari, privi di identificativi e previa richiesta all'Istat, relativi ai territori di rispettiva competenza e necessari per lo svolgimento delle funzioni istituzionali.

Il Garante ha ritenuto preliminarmente opportuno evidenziare che, a seguito di recenti riforme normative sono state sottratte all'ambito di applicazione della disciplina in materia di

protezione dati le informazioni relative a persone giuridiche, gli enti e le associazioni (art. 40, comma 2, del d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214). In tale quadro ha però precisato che anche nei censimenti sull'industria, sui servizi e sulle istituzioni *non profit* possono comunque emergere dati riferibili a persone fisiche (ad es., imprese individuali e liberi professionisti) in relazione ai quali la normativa in materia di protezione dati deve applicarsi.

Ciò premesso, l'Autorità, ha preso positivamente atto delle garanzie individuate nel piano generale di censimento al fine di assicurare il rispetto dei diritti degli interessati (parere 9 febbraio 2012 [doc. web n. 1876517]).

7.2. PROGRAMMA STATISTICO NAZIONALE

Aggiornamenti del Programma statistico nazionale

L'Autorità ha espresso parere favorevole, ma condizionato, sull'Aggiornamento 2012-2013 del Programma statistico nazionale 2011-2013 (art. 6-*bis*, comma 2, d.lgs. n. 322/1989).

Nel parere è stato rilevato con favore che l'Istituto, attuando quanto indicato nel precedente parere (provv. 23 settembre 2010 [doc. web n. 1753181]), ha evidenziato che i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati, trattati per finalità che non richiedono il loro utilizzo.

Alcune criticità sono state riscontrate in relazione a due specifiche indagini, sulla sicurezza della donna e sulla sicurezza dei cittadini, con riferimento alla mancata indicazione, nei relativi prospetti identificativi, dei dati sulla vita sessuale oggetto di rilevazione.

In particolare, l'indagine sulla sicurezza della donna, di indiscussa utilità sociale, prevede la formulazione di numerosi quesiti riguardanti dati sensibili che rilevano aspetti particolarmente intimi e privati della vita delle donne intervistate. In tale quadro il Garante, nel condizionare il parere all'opportuna integrazione dei predetti prospetti identificativi con l'indicazione dei dati sulla vita sessuale, ha raccomandato sia che, nella realizzazione dell'indagine fosse -anche prima dell'intervista- rappresentato alle interessate che non sussiste obbligo di fornire informazioni aventi carattere sensibile e giudiziario, sia che gli intervistatori, possibilmente donne, fossero adeguatamente formati ed eventualmente affiancati da psicologi (parere 21 luglio 2011 [doc. web n. 1829659]).

Nel 2012, inoltre, su richiesta dell'Istat l'Autorità si espressa in relazione al trattamento di dati personali inseriti per la prima volta nel Psn 2011-2013, Aggiornamento 2013, e alle modifiche apportate ai prospetti identificativi di lavori statistici già inclusi nel precedente Psn 2011-2013 e nel relativo Aggiornamento 2012-2013 (parere 9 febbraio 2012 [doc. web n. 1876517]).

In primo luogo, il Garante ha preso atto del mancato adeguamento alle modifiche normative che hanno sottratto all'ambito di applicazione della disciplina in materia di protezione dati le informazioni relative a persone giuridiche, enti e associazioni. Tale circostanza è stata motivata dall'Istituto in ragione sia del fatto che le predette modifiche sono intervenute nella fase conclusiva dell'*iter* di approvazione del programma, sia della difficoltà di operare, in certi casi, una distinzione analitica tra i trattamenti di dati relativi esclusivamente a persone fisiche e quelli relativi a persone giuridiche, enti ed associazioni. Sul punto l'Autorità ha raccomandato, in vista della redazione del Psn 2014-2016, di prestare particolare attenzione a quei lavori statistici che, pur concernendo prevalentemente persone giuridiche, possono comportare il trattamento di dati personali riferiti a persone fisiche (quali quelli relativi ad attività professionali svolte in forma individuale, ovvero quelli relativi a persone giuridiche che comportano l'utilizzo delle cd. "liste di partenza" per contattare i rispondenti recanti i nominativi di persone fisiche). Ciò, anche in relazione all'individuazione delle variabili da diffondere in forma disaggregata, in ragione del fatto che tale modalità di diffusione, riferita a persone giuridiche, può comportare anche il riferimento a dati relativi a persone fisiche (art. 4, comma 2, del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, Allegato A.3. al Codice).

Il Garante ha evidenziato specifiche criticità con riferimento agli studi progettuali del Ministero del lavoro e delle politiche sociali "LPR-00118 progetto sperimentale volto alla creazione e implementazione del sistema informativo sui servizi sociali per le non autosufficienze (SINA)" e "LPR-00128 SINBA-Progetto sperimentale volto alla creazione e implementazione del sistema informativo sulla cura e la protezione dei bambini e della loro famiglia".

Tali studi prevedono, in particolare, che informazioni trattate a fini amministrativi dai comuni siano trasmesse dalle regioni e dalle province autonome al sistema informativo dell'Inps, corredate di dati identificativi diretti e di dati molto delicati relativi anche allo stato di salute e alla vita sessuale. In entrambi i casi tra gli obiettivi dello studio vi sarebbe quello di far confluire i predetti flussi informativi nel Casellario dell'assistenza istituito presso l'Inps ai sensi dell'art.13 del d.l. 31 maggio 2010, n. 78, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 30 luglio 2010, n. 122, le cui modalità di attuazione dovranno essere definite con un decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro dell'economia e delle finanze, nel rispetto del Codice.

In tale quadro, il Garante si è riservato di valutare, nell'ambito del parere di conformità sul decreto attuativo del Casellario dell'assistenza, la compatibilità con la normativa in materia di protezione dati di un'eventuale raccolta centralizzata -con dati identificativi diretti, in un unico sistema- di informazioni così delicate, anche idonee a rivelare lo stato di salute e la vita sessuale, riferite a minori. Ciò, anche con riferimento all'attuazione dei nuovi flussi di dati personali in ambito sociale e assistenziale previsti dall'art. 16 del d.l. 9 febbraio 2012, n. 5, convertito in legge, con modificazioni, dalla l. 4 aprile 2012, n. 35.

In particolare l'Autorità ha evidenziato che i dati personali trattati per scopi statistici non possono essere utilizzati per finalità di altra natura e che i relativi prospetti identificativi non indicano l'assenza dell'obbligo di risposta da parte degli interessati con riferimento ai dati sensibili e giudiziari, il trattamento dei quali, per altro, allo stato non è previsto da alcuna norma di legge che individui i tipi di dati e le operazioni eseguibili.

L'Autorità ha pertanto condizionato il parere favorevole sul Psn 2011-2013, Aggiornamento 2013, all'eliminazione dallo stesso dei predetti studi progettuali del Ministero del lavoro e delle politiche sociali (parere 20 settembre 2012 [doc. web n. 2069239]).

Informativa semplificata

Per la realizzazione del Censimento, l'Istat si è avvalsa delle liste anagrafiche comunali (lac) per acquisire i contatti necessari all'inoltro dei questionari censuari e ridurre il numero di rilevatori impiegati sul campo. In base alla normativa di settore, trattandosi di dati personali non raccolti presso l'interessato, ove il conferimento dell'informativa a quest'ultimo richieda uno sforzo sproporzionato rispetto al diritto tutelato, l'informativa stessa si considera resa se

il trattamento è incluso nel Psn o è oggetto di pubblicità con idonee modalità da comunicare preventivamente al Garante, il quale può prescrivere eventuali misure ed accorgimenti (art. 6, comma 2, del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistan). L'Istat ha dovuto avviare la rilevazione delle liste anagrafiche comunali -una raccolta di dati presso terzi- prima dell'approvazione del Psn 2011-2013 e, pertanto, ha comunicato al Garante di voler pubblicare un'apposita informativa su due giornali a larga diffusione nazionale e su un giornale locale per i cittadini italiani di lingua tedesca della Provincia autonoma di Bolzano. L'Autorità, tuttavia, ha ritenuto che l'informativa dovesse essere pubblicata anche sul sito internet dell'Istat e che dovesse rimanere visibile fino alla pubblicazione del Psn 2011-2013 nella Gazzetta Ufficiale (provv. 19 gennaio 2011 [doc. web n. 1784974]).

Della possibilità di fornire un'informativa semplificata si sono avvalsi nel 2012 anche alcuni soggetti Sistan.

In particolare, il Ministero dell'istruzione, dell'università e della ricerca ha rappresentato all'Autorità di voler realizzare uno studio statistico sul valore degli esiti degli esami di Stato con riguardo all'ingresso degli studenti nelle università, attraverso l'elaborazione di dati già in suo possesso raccolti in banche dati amministrative diverse (nota 2 marzo 2012).

L'Istat, invece, si è avvalso di tale possibilità per alcune notizie relative al ruolo di responsabili del trattamento svolto da alcune regioni compartecipanti al progetto "Sperimentazione di un nuovo flusso di acquisizione dei dati di mortalità"- STU IST 02150, già inserito nel Pns 2011-2013 e nel relativo Aggiornamento 2012-2013 (nota 26 luglio 2012), nonché per comunicare alla Banca d'Italia i nominativi di famiglie campione estratti dalle anagrafi comunali per un'indagine sui bilanci delle famiglie italiane (v. art. 21, comma 2, del Regolamento (CE) n. 223/2009, che autorizza la "trasmissione di dati riservati" da un'autorità del sistema statistico europeo (nella specie, l'Istat) a un membro del sistema europeo delle banche centrali (nella specie la Banca d'Italia) "*a condizione che sia necessaria ai fini dell'efficienza dello sviluppo, della produzione e della diffusione di statistiche europee o del miglioramento della loro qualità" e "che tale necessità sia stata giustificata*"). L'Autorità ha al riguardo precisato che l'origine dei dati trattati dovrà essere

specificata anche nell'informativa che la Banca d'Italia renderà agli interessati nell'ambito dello svolgimento della predetta indagine statistica campionaria sui bilanci delle famiglie italiane (nota 17 dicembre 2012).

Collaborazione con l'Istat

Nel 2012, l'Ufficio ha collaborato con l'Istat per la revisione dei prospetti identificativi dei progetti inseriti nel Psn utilizzati per descrivere il trattamento di dati personali al fine di rendere una corretta informativa agli interessati, con particolare riferimento alla comunicazione dei dati sensibili e giudiziari tra soggetti Sistan.

Infine il Garante ha manifestato all'Istat la propria disponibilità a partecipare alla revisione del d.lgs. n. 322 del 1989 e al complessivo riordino del Sistema statistico nazionale cui l'Istituto si accinge alla luce di recenti modifiche normative (nota 27 novembre 2012).

8. L'attività di polizia

8.1. Il controllo sul Ced del Dipartimento della pubblica sicurezza

A seguito di segnalazioni ricevute, l'Autorità ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici della polizia di Stato alle richieste degli interessati sia di accesso e comunicazione dei dati conservati presso il Centro elaborazione dati (Ced), sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni poste dall'art. 10 della l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8.2. Altri interventi in relazione ad attività di forze di polizia

Nel 2012 si è conclusa una complessa istruttoria avviata a seguito di un quesito posto dal legale rappresentante di una struttura operante nel campo del recupero e reinserimento di soggetti tossicodipendenti, concernente la richiesta proveniente da un Comando dell'Arma dei Carabinieri di inviare l'elenco di tutte le persone accolte presso la struttura.

All'esito dell'istruttoria, esaminate le fonti normative, il Garante ha comunicato al rappresentante della struttura e al Comando dell'Arma che non risultava sussistere una base normativa idonea a giustificare la trasmissione sistematica al Comando dell'elenco delle persone ricoverate presso la comunità terapeutica, rilevando che tali informazioni possono essere legittimamente acquisite unicamente a puntuale evasione di richieste provenienti dall'autorità giudiziaria, finalizzate al controllo dei soggetti sottoposti a misure restrittive ed alternative della libertà personale eventualmente soggiornanti presso la comunità (nota 26 gennaio 2012).

È altresì pervenuta al Garante una segnalazione con la quale veniva riferito che un agente di polizia in borghese aveva effettuato videoriprese nel corso di una manifestazione, dall'esterno del corteo, nel quale si era successivamente inserito, effettuando riprese a distanza ravvicinata e captando anche suoni e conversazioni.

Il commissariato interessato, nel riscontrare la richiesta di chiarimenti dell'Autorità, ha precisato che, trattandosi di manifestazione non autorizzata, le riprese come previsto in tali circostanze, erano finalizzate unicamente a individuare eventuali autori di reati. Nel caso di specie le riprese avevano consentito di identificare una persona, nei cui confronti era stato

promosso un procedimento penale e che era stata rinviata a giudizio, quale autore di un'aggressione ai danni di un operatore di polizia. Il commissariato ha altresì chiarito che le riprese erano state dirette a riprendere le fasi dei tafferugli e non per captare anche suoni e conversazioni, e che le eventuali tracce sonore di sottofondo rilevate in tali circostanze non erano riconducibili a persone definite.

Sulla base di tali chiarimenti il Garante non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali nell'attività posta in essere dagli agenti, rientrante nell'ambito dei trattamenti effettuati dalle forze di polizia, ai sensi degli artt. 53 e ss. del Codice, per finalità di tutela dell'ordine e della sicurezza pubblica (nota 4 maggio 2012).

Non sono emerse violazioni neppure riguardo ad una segnalazione con cui veniva riferito che le postazioni informatiche presenti nella sala intercettazione di un comando dell'Arma dei Carabinieri risultavano sprovviste di *password* e che conseguentemente era possibile per chiunque si trovasse nella sala accedere liberamente alla documentazione ivi presente. Nel caso di specie, il segnalante, in servizio presso il comando dell'Arma, aveva avuto casualmente accesso ad un documento contenente una relazione di servizio che lo riguardava.

Il Comando, interpellato dall'Autorità, ha chiarito che la postazione informatica in questione, collegata ad una rete protetta e dotata di antivirus ad aggiornamento automatico, non era utilizzata per attività di intercettazione, ma era posta a disposizione del personale operante nella sala per ricerche di carattere personale su internet. Gli altri apparati presenti nella sala, utilizzati per attività di intercettazione, erano invece accessibili solo mediante procedure di autenticazione. Il Comando ha aggiunto che anche nel procedimento penale instaurato su denuncia-querela dell'interessato, conclusosi con un decreto di archiviazione, era stato accertato che l'evento rappresentato dal segnalante si era verificato su di una postazione non utilizzata per attività di intercettazione, e che era riconducibile ad un automatismo indotto da un *software* installato nel computer (nota 16 novembre 2012).

Accesso della polizia giudiziaria a dati sensibili

Un ufficio periferico dell'Inps ha chiesto a questa Autorità di conoscere le corrette modalità di comportamento in caso di richieste della polizia giudiziaria, finalizzate alla prosecuzione delle indagini, di accesso ai dati personali contenuti nei verbali di invalidità civile contenenti l'indicazione delle patologie.

Il Garante ha ricordato che tale ipotesi è regolata dall'art. 25, comma 2, del Codice -applicabile anche ai trattamenti effettuati dai soggetti pubblici, in base al rinvio di cui all'art. 18, comma 5, del Codice stesso- che, tra l'altro, consente la comunicazione di dati richiesti, in conformità alla legge, dalle forze di polizia per finalità di prevenzione, accertamento o repressione di reati (nota 21 novembre 2012).

Accertamento della situazione economica del debitore prodromica a procedura esecutiva

Un cittadino aveva segnalato di essere stato convocato da un commissariato della polizia di Stato, in quanto debitore delle spese di giudizio relative ad un contenzioso con una pubblica amministrazione, al fine di acquisire notizie sulla sua situazione economica, in previsione dell'eventuale promozione di una procedura esecutiva a suo carico.

Al riguardo il Garante ha osservato che l'ordinamento giuridico prevede appositi strumenti per consentire al creditore esecutante di individuare i beni del debitore da sottoporre a pignoramento (v. art. 492, comma 7, c.p.c.), mentre tra i compiti istituzionali della polizia di Stato non rientra il compimento delle suddette indagini; né, nella specie, risulta applicabile l'art. 53 del Codice, che ha riguardo al trattamento di dati personali effettuato per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, nella specie non ricorrenti.

Né il trattamento né la comunicazione dei dati all'ente pubblico esecutante risultavano quindi previsti da idonea base normativa, ovvero rientranti nelle funzioni istituzionali della polizia, sicché sono risultati violati gli artt. 18, comma 2 e 19 comma 2, del Codice.

Per questi motivi il Garante ha dichiarato illecito il trattamento e vietato, ai sensi degli artt. 143, comma 1, lett. *c)* e 154, comma 1, lett. *d)*, del Codice, ogni ulteriore operazione di trattamento di tali dati da parte del commissariato e dell'ente pubblico creditore, salva la valutazione della sussistenza dei presupposti per la contestazione di violazioni amministrative (provv. 4 ottobre 2012).

8.2.1. Acquisizione di dati da parte delle forze di polizia

Nel 2012 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 per via telematica delle forze di polizia a due importanti banche dati.

Il primo parere era stato richiesto dal Dipartimento della pubblica sicurezza del Ministero dell'interno in ordine a uno schema di Convenzione avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (Ced) del Dipartimento, alla banca dati dell'Inps, attraverso l'utilizzo di specifiche applicazioni informatiche. In entrambi i casi i testi sono stati definiti sulla base di approfondimenti svolti dall'Autorità con le parti, in un clima di piena collaborazione, per assicurare il rispetto, anche sotto il profilo della sicurezza, delle norme sulla protezione dei dati personali.

La prima richiesta è risultata fondata sulla normativa (l. 31 maggio 1965, n. 575, confluita nel codice delle leggi antimafia d.lgs. n. 159/2011) 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.

A tali fini il questore può richiedere ad ogni ufficio della p.a., ad imprese, società ed enti di ogni tipo, informazioni e copia della documentazione ritenuta utile.

Il testo definisce in particolare quali dati siano oggetto della Convenzione (dati anagrafici, retributivi, contributivi e pensionistici dei soggetti censiti dall'Inps), le finalità dell'accesso (esclusivamente quelle connesse allo svolgimento delle attività previste dalla suddetta normativa) ed il personale ad esso abilitato (operatori delle forze di polizia con qualifica di ufficiale o agente di polizia giudiziaria), cui dal Ced sono attribuiti specifici profili di abilitazione e credenziali di autenticazione personali ed impartite direttive relative alle responsabilità connesse all'uso illegittimo delle informazioni.

È altresì previsto, per entrambe le parti, l'obbligo di formazione di detto personale all'utilizzo della banca dati; sono stati configurati specifici divieti a carico del Ced, 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 sottopone l'accesso alla banca dati dell'Istituto ai sistemi per il monitoraggio degli

accessi e di *alert* su anomalia in uso al Centro; i risultati di tali attività sono resi disponibili per i capi degli uffici per trenta giorni nel portale del Ced.

Il testo indica la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla convenzione.

L'Autorità ha, peraltro, subordinato il proprio parere favorevole sulla Convenzione:

- alla riformulazione della nozione di "dato personale" alla luce delle modifiche che hanno sottratto le persone giuridiche, gli enti e le associazioni dall'ambito di applicazione della disciplina in materia di protezione dei dati personali (art. 4 del Codice, v. art. 40, comma 2, del d.l. 6 dicembre 2011, n. 201 convertito dalla l. 22 dicembre 2011, n. 214);

- all'indicazione che l'allegato B. della Convenzione, contenente l'analitica elencazione dei dati consultabili, costituisce parte integrante della medesima (parere 2 febbraio 2012 [doc. web n.1875293]).

Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze

Il secondo parere ha riguardato la Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (Ced) del Dipartimento della pubblica sicurezza, ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf) gestito dall'Ufficio centrale antifrode dei mezzi di pagamento (Ucamp) del Ministero dell'economia e delle finanze (v. norme sull'accesso del Dipartimento della pubblica sicurezza alle informazioni e ai dati contenuti nel sistema di prevenzione delle frodi sulle carte di pagamento l. 17 agosto 2005, n. 166 e del d.m. del Ministero dell'economia e delle finanze 30 aprile 2007, n. 112).

Anche in questo caso il testo individua specificamente le tipologie di dati e di informazioni oggetto della convenzione (attraverso il riferimento all'elenco contenuto negli artt. 6 e 7 del citato d.m. n. 112/2007); delimita le finalità dell'accesso (solo la prevenzione e repressione dei reati connessi all'utilizzo di carte di credito o di altri mezzi di pagamento) (v. parere reso dal Garante il 19 ottobre 2006 sullo schema del decreto attuativo della l. n. 166/2005 [doc. web n. 1353472]), riservato agli operatori delle forze di polizia cui sono attribuiti dal Ced specifici profili di abilitazione e credenziali di autenticazione personali.

È posto l'obbligo per il Ced di 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.

Sono stati previsti specifici divieti a carico del Ced, 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, viene specificato che gli utenti accedono al Sipaf esclusivamente tramite VPN (*Virtual Private Network*) *site to site* su rete *SPC* con protocollo "*IPsec/tunnel*", utilizzando inoltre il protocollo "ssl" per garantire le funzionalità di crittografia dei dati trasferiti tra *client* e *server*.

È previsto che il Ced provvede al tracciamento delle attività all'interno del suo dominio di applicazione, mentre l'applicativo Sipaf provvede al tracciamento delle operazioni svolte dagli utenti.

Il Ced sottopone l'accesso alla banca dati Sipaf ai sistemi per il monitoraggio degli accessi e di *alert* su anomalia in uso al Centro; i risultati di tali attività sono resi disponibili per i capi degli uffici per trenta giorni nel portale del Ced.

Il testo indica, infine, la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla convenzione.

Poiché tali modalità 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 12 luglio 2012 [doc. web n. 1915461]).

8.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle ultime misure 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 che verranno introdotte con la prossima 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.

Alla luce delle indicazioni ricevute e delle difficoltà rappresentate dal Ministero, il Garante ha differito i termini per l'adempimento delle prescrizioni, che sono in corso di attuazione (provv. 24 gennaio 2013 [doc. web n. 2324763]).

Accesso diretto

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

Sono invece rimaste sostanzialmente stabili 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.

9. L'attività giornalistica

9.1. Minori

Anche nel periodo di riferimento non sono mancate occasioni di valutare come si atteggia in concreto il delicato rapporto tra la libertà di informazione e il diritto alla riservatezza e alla protezione dei dati dei minori, che ha come principale quadro di riferimento il Codice (artt. 50 e 136 e ss), il codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, riportato nell'Allegato A.1. del Codice (in particolare all'art. 7) e la Carta di Treviso.

Le disposizioni citate, oltre a richiedere il rispetto dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, prevedono che il diritto del minore alla riservatezza deve sempre essere considerato come primario rispetto al diritto di cronaca. Le medesime disposizioni prevedono altresì espressamente che, al fine di tutelarne la personalità, i giornalisti non rendano identificabili i minori coinvolti in fatti di cronaca.

Il Garante ha invocato tali princìpi nel caso relativo all'attentato di Brindisi, invitando gli organi di informazione e i siti web ad astenersi dalla pubblicazione di dettagli e immagini lesivi della dignità della minorenne deceduta, raccomandando, inoltre, particolare attenzione e senso di responsabilità nell'utilizzare foto messe in rete dai minori per condividere momenti della loro vita.

Analogo richiamo è stato effettuato dall'Autorità per la vicenda della bambina deceduta in un tragico incidente su una spiaggia francese, in questo caso anche al fine di tutelare gli altri minori componenti della famiglia della vittima (v. rispettivamente comunicati stampa 19 maggio e 28 agosto 2012 [doc. web nn. 1894787 e 1921070]).

Tanto più è necessaria la sensibilizzazione sul tema cronaca e minori e il rispetto delle garanzie sopra richiamate ove si consideri la diffusione illimitata (e talora dirompente) del web rispetto alle notizie di cronaca. Così è stato per il caso delle immagini e dei dati personali relativi al bambino di Padova prelevato a scuola dalle forze di polizia, in esecuzione di un provvedimento giurisdizionale di affidamento (comunicato stampa 11 ottobre 2012 [doc. web n. 2058275]).

Nell'ambito di alcuni riscontri forniti su segnalazioni pervenute nel corso dell'anno riguardanti la diffusione di immagini riferite a minori di età, l'Autorità, richiamando quanto affermato nel documento del 6 maggio 2004 "*Privacy* e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti" [doc. web n. 1007634], ha sottolineato che la diversità del contesto all'interno del quale possono essere raccolte e successivamente diffuse informazioni riguardanti i minori può influire significativamente sulla complessiva valutazione della pubblicazione stessa. In particolare, può risultare lecita la diffusione di immagini che danno positivo risalto a qualità del minore o che lo rappresentano in momenti di svago o di gioco (nota 29 agosto 2012).

9.2. CRONACHE GIUDIZIARIE

Nel 2012 una parte significativa delle richieste di intervento rivolte al Garante ha riguardato il trattamento di dati personali nell'ambito della cronaca giudiziaria che -nel necessario bilanciamento tra libertà di espressione, tutela della riservatezza e della dignità delle persone, anche alla luce dei princìpi di non colpevolezza sino alla sentenza definitiva e di rieducazione del condannato- deve conformarsi sia alle disposizioni di cui agli artt. 136-139 del Codice, sia al codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica.

9.2.1. Pubblicazione di intercettazioni

L'applicazione dei suddetti princìpi impone particolari cautele in caso di pubblicazione di intercettazioni effettuate nell'ambito di procedimenti giudiziari, anche alla luce della specifica aspettativa di riservatezza riconosciuta a coloro che sono impegnati in una conversazione telefonica o in altra forma di comunicazione in ambito privato.

In concreto, risulta spesso difficile per il Garante, sulla base della documentazione disponibile, valutare la conformità di specifiche pubblicazioni alla disciplina in materia di segreto investigativo e divieto di pubblicazione di atti del procedimento penale. Anche alla luce di ciò, a fronte di un reclamo presentato da un componente parlamentare avverso la diffusione attraverso la rete internet del testo di un'informativa contenente la trascrizione di

numerose intercettazioni telefoniche che lo riguardavano, il Garante ha chiesto la collaborazione della procura della Repubblica competente per le relative indagini, al fine di accertare se il materiale oggetto di diffusione fosse o meno coperto da segreto (nota 18 dicembre 2012).

In un diverso caso, invece, l'Autorità ha ritenuto che non fosse stato travalicato il limite dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico, in quanto la pubblicazione della notizia che una determinata utenza telefonica fosse stata sottoposta ad intercettazione era giustificata dalla presenza di rapporti tra l'intestatario dell'utenza e persone a diverso titolo legate ad una complessa indagine giudiziaria. Pertanto il Garante, anche alla luce del fatto che gli articoli giornalistici oggetto di segnalazione, al momento dell'accertamento dell'Ufficio, non risultavano rintracciabili all'interno dei motori di ricerca, ha ritenuto non vi fossero gli estremi per adottare provvedimenti di carattere inibitorio (nota 4 gennaio 2013).

9.2.2. Informazioni relative a procedimenti

Notizie e immagini di arrestati e indagati

L'Autorità ha fornito riscontro 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.).

Su tali basi sono state ritenute prive di fondamento diverse segnalazioni concernenti l'avvenuta pubblicazione dei nomi di persone indagate, imputate o condannate, effettuata nel rispetto dei princìpi posti dal Codice, in particolare dall'art. 137, comma 3 e dal codice di deontologia cit. (nota 29 agosto 2012).

L'Autorità ha d'altra parte confermato il proprio consolidato orientamento a tutela della dignità delle persone sottoposte a procedimento penale con il provvedimento 18 maggio 2012 [doc. web n. 1900914], in relazione alla segnalazione di un caso che presenta aspetti

di novità rispetto ad ipotesi prese in considerazione in passato. In particolare, nell'ambito di una trasmissione televisiva riconducibile al cd. "giornalismo di inchiesta", erano state diffuse immagini raccolte da agenti operanti in funzione di polizia giudiziaria, che in una irruzione notturna perquisivano gli appartamenti di alcuni indagati, procedendo alle operazioni di arresto.

Nel ritenere che il servizio televisivo avesse, in termini generali, lecitamente riferito gli esiti delle indagini coordinate dalla Direzione distrettuale antimafia, dando anche conto dei dati identificativi delle persone ad esse sottoposte, il Garante ha, invece, disposto il divieto dell'ulteriore diffusione delle immagini in chiaro riferite a queste ultime, ritratte all'interno delle proprie abitazioni private -anche attraverso l'utilizzo di cd. "primi piani"- nel momento delicatissimo della presa in consegna da parte delle forze dell'ordine, ritenendo che ciò avesse travalicato i limiti posti dall'ordinamento all'esercizio del diritto di cronaca, in particolare il principio di tutela della dignità della persona e il principio di essenzialità dell'informazione rispetto a fatti di interesse pubblico.

L'Autorità, inoltre, sempre a tutela della dignità delle persone arrestate, ha adottato un provvedimento inibitorio nei confronti di una maestra d'asilo arrestata per maltrattamento a danni di minori. L'immagine della stessa, al momento dell'arresto, infatti, veniva trasmessa nel corso di alcuni servizi giornalistici di telegiornali in relazione ad episodi di maltrattamenti a danno di minori non imputabili alla reclamante. Il Garante ha quindi ritenuto che, in tali casi, l'uso della suddetta immagine non potesse ritenersi essenziale rispetto alla finalità di fornire informazioni su un diverso episodio (provv. 5 giugno 2012 [doc. web n. 1912974]).

Vittime di reato, testimoni e persone estranee ai fatti

Il richiamato parametro dell'"*essenzialità dell'informazione*" ha costituito il principio-guida di riferimento nella valutazione di 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); oppure riguardavano fatti che, pur essendo relativi alle persone indagate, risultavano essere estranei ai fatti oggetto di indagine.

In particolare il Garante, nell'esaminare alcuni reclami e segnalazioni in argomento, ha ribadito che nel trattamento di dati e immagini relativi a persone vittime di episodi

criminosi, il rispetto dell'"*essenzialità dell'informazione*" va assicurato con particolare rigore, anche quando le notizie riguardino vittime decedute.

Tali garanzie (che trovano riscontro anche nel quadro giuridico europeo: cfr. Raccomandazione (2003)13 del Comitato dei ministri del Consiglio d'Europa del 10 luglio 2003 "Princìpi relativi alle informazioni fornite attraverso i mezzi di comunicazione in rapporto a procedimenti penali") sono state richiamate, fra l'altro, a fronte della diffusione, da parte di alcuni giornali e siti di informazione, di immagini tratte dalla perizia medico legale effettuata sul corpo di una donna, che il Garante ha ritenuto eccedenti rispetto alla finalità informativa e lesive della dignità dell'interessata (note 9 agosto e 8 novembre 2012).

Le medesime garanzie di tutela sono state alla base della valutazione di una segnalazione relativa ad alcuni servizi giornalistici riguardanti il nuovo filone di indagine sulla morte di una giovane studentessa di Brembate, relativamente al possibile coinvolgimento di un uomo, poi defunto (le cui tracce di Dna lo qualificherebbero quale padre naturale del possibile omicida) e dei suoi familiari (autori della segnalazione). L'Autorità ha infatti ritenuto eccedente la pubblicazione della fotografia del defunto apposta sulla lapide nonché una serie di informazioni relative ai suoi familiari (dati anagrafici, di residenza e credo religioso) pubblicate, in particolare, da un quotidiano locale. Ciò, considerato che si trattava di un'ipotesi investigativa discussa, ancora alla fase iniziale, e che era emersa da subito l'estraneità del defunto e dei familiari citati dal giornale rispetto all'omicidio della giovane (nota 13 dicembre 2012).

Il Garante ha altresì ritenuto fondata la segnalazione di una donna che aveva lamentato una possibile lesione della sua *privacy* e della sua sicurezza personale in ragione della pubblicazione, all'interno di un quotidiano, della prima parte del verbale della sua deposizione quale "*persona informata di fatti*" oggetto di un procedimento penale. La riproduzione fotografica, con caratteri leggibili e senza alcuna forma di mascheramento, di parte di questo verbale aveva infatti reso conoscibili alcuni dati della segnalante (in particolare la data e il luogo di nascita nonché la attuale residenza, comprensiva di via e numero civico) che il Garante ha ritenuto non essenziali ai fini della completezza informativa sulla vicenda di interesse pubblico oggetto di quel procedimento penale (nota 16 luglio 2012).

9.3. PERSONAGGI PUBBLICI

L'Autorità è stata nuovamente chiamata ad affrontare la questione della raccolta e diffusione di informazioni riguardanti personaggi pubblici o persone che esercitano pubbliche funzioni. Come evidenziato nelle precedenti relazioni annuali, il quadro normativo e l'evoluzione giurisprudenziale in materia consentono di individuare margini più ampi nel trattamento dei dati personali relativi a siffatte figure. Lo stesso codice di deontologia stabilisce che "*la divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata sia indispensabile in ragione della….qualificazione del protagonista*" (art. 6, comma 1).

Dallo stesso codice si evince altresì che informazioni riguardanti personaggi pubblici, anche relative alla loro sfera privata, possono essere divulgate se assumono rilievo sul loro ruolo o sulla loro vita pubblica (art. 6, comma 2), ovvero se tratte da dichiarazioni o comportamenti pubblici degli stessi interessati (art. 137, comma 3 del Codice). Anche in tale ambito vanno comunque rispettati l'essenzialità dell'informazione e la dignità della persona (artt. 10 e 11 del codice di deontologia).

In tale quadro normativo l'Autorità ha ritenuto leciti alcuni articoli, oggetto di segnalazione, relativi al ricovero della presidente di una regione in una struttura sanitaria, per un intervento. Il Garante non ha rinvenuto in essi dettagli relativi alla patologia o al tipo di intervento subito o altre informazioni eccedenti; d'altra parte ha riscontrato che gli articoli facevano riferimento a una questione da cui aveva preso le mosse anche un'interrogazione consiliare e di cui non poteva non riconoscersi una rilevanza pubblica. Il Garante ha poi riscontrato che gli organi di informazione avevano dato anche ampia evidenza ai successivi chiarimenti dell'interessata sulla vicenda (nota 11 ottobre 2012).

I limiti sopra ricordati sono stati invece richiamati dal Garante in merito a un reclamo concernente la pubblicazione di servizi giornalistici relativi ad un'asserita relazione sentimentale tra due personaggi dello spettacolo, desumibile da uno scambio di sms, poi prodotti in un procedimento giudiziario. In particolare il Garante ha prescritto agli organi di informazione di astenersi dalla pubblicazione di sms eventualmente idonei a rivelare abitudini sessuali (art. 11 codice di deontologia) (provv. 13 dicembre 2012 [doc. web n. 2142715]).

Il Garante -su segnalazione del direttore di una testata televisiva- è stato altresì chiamato ad esprimersi sulla liceità della registrazione, da parte di un giornalista di un noto quotidiano a tiratura nazionale, di una comunicazione telefonica intercorsa tra il giornalista stesso e il segnalante, cui ha fatto seguito la pubblicazione del contenuto della conversazione sul quotidiano. Al riguardo l'Autorità ha in particolare precisato che la consapevolezza dell'interlocutore che la conversazione telefonica venisse utilizzata per finalità giornalistiche avrebbe dovuto essere valutata considerando la particolare qualificazione dei protagonisti, entrambi esperti dei meccanismi del mondo dell'informazione e figure note in tale ambito. La successiva pubblicazione del contenuto della conversazione da parte del quotidiano è stata poi ritenuta riconducibile a temi di interesse pubblico -rientrando in un'accesa polemica, a cui aveva preso parte anche il quotidiano stesso, riguardante i contenuti di una discussa serie televisiva, trasmessa dal direttore della testata (segnalante) e poi interrotta per decisione dei vertici aziendali- riferiti, in termini complessivamente essenziali. Peraltro a seguito della presentazione della segnalazione, il quotidiano ha autonomamente rimosso dal proprio sito internet il *file* audio contenente la registrazione della telefonata (nota 7 settembre 2012).

L'Autorità ha altresì risposto ad un assessore comunale, circa la liceità della diffusione, senza il suo consenso, di foto che la riguardavano nell'ambito di un articolo di un quotidiano locale dal titolo "I politici spiati sui *social network*". Gli elementi disponibili non hanno evidenziato specifici elementi di illiceità nell'acquisizione della fotografia, scattata in luoghi pubblici ed acquisita dal profilo Facebook della segnalante ad opera del giornalista che risultava essere stato suo "amico su Facebook". La diffusione della fotografia inoltre risultava essere avvenuta nei limiti previsti dalle disposizioni deontologiche riferibili a figure di pubblico rilievo (art. 6 cit.). L'Autorità ha comunque rappresentato all'interessata la possibilità di opporsi all'ulteriore trattamento dei propri dati per motivi legittimi (art. 7, comma 4, lett. *a)* del Codice e, in termini più specifici, art. 5, comma 2 del codice di deontologia relativo ai trattamenti a fini giornalistici) (nota 26 luglio 2012).

9.4. USO DI IMMAGINI IN AMBITO GIORNALISTICO

Il trattamento per finalità giornalistiche di immagini di persone identificabili, poste a corredo di servizi giornalistici, ha costituito oggetto di due provvedimenti del Garante adottati a seguito della presentazione di reclami.

In entrambi i casi le immagini riconoscibili di dipendenti di istituzioni pubbliche (non inquadrabili nella categoria delle cd. "persone note"), ritratti mentre attendevano ai propri compiti all'interno di un'aula parlamentare, erano state associate, rispettivamente, ad un articolo pubblicato su un quotidiano nazionale e a un servizio televisivo.

L'Autorità ha deciso, tenendo distinti i due casi, che -se è legittima la pubblicazione di immagini, purché lecitamente raccolte, finalizzata alla individuazione visiva degli appartenenti a categorie il cui trattamento giuridico ed economico è oggetto di un dibattito pubblico (provv. 15 novembre 2012 [doc. web n. 2247923])- non è invece legittima la proposizione -anche attraverso l'utilizzo di particolari tecniche- di immagini individualizzate del singolo, il quale viene in tal modo presentato quasi come "emblema" di un'intera categoria.

Nel caso specifico, tuttavia, non si è adottato alcun provvedimento inibitorio, considerata la decisione spontanea del titolare del trattamento di non utilizzare più le predette immagini (provv. 15 novembre 2012 [doc. web n. 2185342]).

9.5. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

Anche nel 2012 il Garante ha ricevuto diverse segnalazioni e ricorsi concernenti la reperibilità, a distanza di anni, di dati personali a suo tempo pubblicati su quotidiani, rinvenibili negli archivi storici dei giornali *online*.

Il Garante ha, al riguardo, ribadito che la diffusione sul sito internet di un quotidiano *online* di un articolo contenente informazioni su fatti anche molto delicati e piuttosto risalenti nel tempo costituisce parte integrante dell'archivio storico della testata e non integra un illecito trattamento di dati personali.

Tuttavia, l'Autorità tenuto conto 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 spesso comportare un sacrificio sproporzionato dei suoi diritti.

L'Autorità, in alcuni provvedimenti, ha richiesto 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 deindicizzata, cioè sottratta alla diretta individuazione attraverso i comuni motori di ricerca, pur restando tale pagina inalterata nel contesto dell'archivio e consultabile telematicamente accedendo all'indirizzo web dell'editore (provv.ti 12 aprile 2012 [doc. web n. 1894581]; 19 luglio 2012 [doc. web n. 2065905]; 4 ottobre 2012 [doc. web n. 2104293]; 18 ottobre 2012 [doc. web n. 2130029]).

Oltre a ribadire queste indicazioni, il Garante ha avviato una rimeditazione del proprio orientamento riguardo al tema dell'aggiornamento delle notizie riportate negli archivi *online* dei quotidiani, anche alla luce di una recente sentenza della Cassazione civile (n. 5525/2012), in base alla quale l'editore *online* -o, comunque, il titolare del sito internet a contenuto informativo- è tenuto ad aggiornare, o almeno a contestualizzare, tutte le notizie pubblicate che riguardino un determinato soggetto. Solo così, infatti, secondo la Suprema Corte, la notizia risulterebbe "*non violativa sia del diritto all'identità personale o morale del titolare, nella sua proiezione sociale del dato oggettivo di informazione e di trattamento, sia dello stesso diritto del cittadino utente a ricevere una completa e corretta informazione*".

In seguito a tale pronuncia l'Autorità ha adottato due provvedimenti (20 dicembre 2012 [doc. web n. 2286432] e 24 gennaio 2013 [doc. web n. 2286820]), nei quali ha riconosciuto il diritto dell'interessato "*ad ottenere l'aggiornamento/integrazione dei dati personali che lo riguardano quando eventi e sviluppi successivi (adeguatamente documentati) hanno modificato le situazioni oggetto di cronaca giornalistica (seppure a suo tempo corretta) incidendo significativamente sul profilo e l'immagine dell'interessato*". Diritto che è stato qualificato come "*indispensabile corollario della riconosciuta liceità della conservazione degli articoli di cronaca a suo tempo pubblicati*" in internet come archivi storici e che va garantito dall'Autorità in quanto "*pienamente compreso fra le posizioni giuridiche azionabili ai sensi dell'art. 7 del Codice*".

In entrambi i provvedimenti l'Autorità ha prescritto all'editore titolare del trattamento di predisporre, nell'ambito dell'archivio storico *online* del quotidiano, un sistema idoneo a

segnalare (ad es., a margine dei singoli articoli o in nota agli stessi) l'esistenza degli sviluppi delle notizie relative ai ricorrenti (coinvolti in un'inchiesta giudiziaria poi conclusasi con l'assoluzione o con la prescrizione del reato).

9.6. PERSISTENTE RINTRACCIABILITÀ SU MOTORI DI RICERCA

Ulteriori interventi dell'Autorità si sono resi necessari al fine di assicurare il rispetto di provvedimenti in cui era stato imposto il divieto di indicizzazione di notizie contenute negli archivi *online*.

Come rappresentato nella Relazione 2011 (p. 91), un editore ha infatti segnalato a questa Autorità, che nonostante l'adozione di tutte le misure tecniche previste, dopo una prima fase in cui la deindicizzazione era parsa efficace, alcuni contenuti risultavano riproposti e visualizzabili nell'indice di Google *search*, talvolta con l'indicazione dell'indisponibilità del sommario proprio a causa dell'applicazione degli strumenti di esclusione.

Con riferimento a tali casi, il Garante ha chiesto a Google chiarimenti; l'istruttoria è in corso.

10. Il trattamento di dati personali attraverso internet

Il crescente utilizzo di internet nelle relazioni economiche e sociali si riflette nell'eterogenea casistica affrontata dall'Autorità.

Trattamento dati *online* per la prenotazione di voli e alberghi

Similmente agli anni precedenti, l'attività dell'Autorità nel 2012 ha riguardato anche il trattamento dati da parte di alcune note società specializzate nella prenotazione *online* di viaggi, alberghi e voli.

In particolare, una segnalazione ha riguardato il trattamento dei dati della carta di credito da parte di un noto sito internazionale, per la ricerca e prenotazione di alloggi in tutto il mondo. Al riguardo, non sono stati ravvisati gli estremi per un intervento dell'Ufficio, poiché la richiesta all'utente interessato dei dati della carta di credito, per la prenotazione *online* di un albergo, è stata ritenuta compatibile con i princìpi di proporzionalità e non eccedenza dei dati personali trattati rispetto alle finalità perseguite (art. 11 Codice) (nota 24 ottobre 2012).

Forum e *blog* dedicati alla salute

Si è riferito nella Relazione 2011 (p. 94), delle linee-guida varate dal Garante (provv. 25 gennaio 2012, in G.U. 20 febbraio 2012, n. 42 [doc. web n. 1870212]) per i siti web dedicati alla salute che non forniscano servizi di assistenza sanitaria *online* o telemedicina, allo scopo di elevare il livello di tutela per chi è iscritto a *social network*, partecipa a *blog* e a *forum* di discussione o segue siti web che si occupano principalmente di tematiche sanitarie.

10.1. Pluralità di trattamenti, diffusione di dati e consenso dell'interessato

Nel corso dell'istruttoria, aperta sulla base di una segnalazione, nei confronti di una nota società di formazione e di preparazione degli esami universitari, è emerso, in particolare che la società in questione raccoglieva dati degli utenti, oltre che per le finalità contrattuali, anche per l'invio di comunicazioni commerciali e materiale pubblicitario, peraltro anche con modalità automatizzate, richiedendo tuttavia un consenso preimpostato, senza acquisirne uno specifico per la finalità promozionale.

Inoltre, la società condizionava la registrazione al sito da parte degli utenti, e conseguentemente anche la fruizione dei servizi in questione, al rilascio del consenso al trattamento per la finalità promozionale.

L'Autorità, con riferimento a precedenti interventi in materia (cfr. provv. 15 luglio 2010 [doc. web n. 1741998] e provv. 11 ottobre 2012 [doc. web n. 2089777]), ha ribadito che non può definirsi "libero" il consenso a ulteriori trattamenti di dati personali che l'interessato "debba" prestare per conseguire una prestazione richiesta, e che l'interessato stesso deve essere messo in grado di esprimere consapevolmente e liberamente il proprio consenso in ordine al trattamento dei dati che lo riguardano, per ciascuna distinta finalità perseguita dal titolare (cfr. provv. 24 febbraio 2005, punto 7. [doc. web n. 1103045]. È stato quindi adottato un provvedimento inibitorio e prescrittivo, ed aperto un autonomo procedimento sanzionatorio (provv. 20 dicembre 2012 [doc. web n. 2223607]).

L'Ufficio ha ravvisato analoghe problematiche per altri siti web, per i quali, tuttavia, ha ritenuto non vi fossero i presupposti per l'adozione di specifici provvedimenti, poiché i titolari, nel dare riscontro alle richieste di informazioni rivolte loro, hanno contestualmente e spontaneamente modificato il tipo di informativa rilasciata ai loro utenti e soprattutto il *form* di acquisizione del consenso, richiedendo una specifica autorizzazione per ciascun tipo di trattamento dati diverso dalle mere finalità contrattuali o da quelle strettamente collegate ad esse.

Diffusione di proposte di acquisto

Una segnalazione lamentava, da parte di una nota compagnia telefonica, la divulgazione *online* senza consenso di alcuni dati personali, fra i quali il nome e cognome, indirizzo, numeri di telefono mobile e/o fisso, di migliaia di clienti, contenuti in altrettante proposte di acquisto (pda).

Nell'istruttoria condotta, la società ha ammesso la divulgazione sul web per alcuni mesi dei dati, riconoscendo che l'accesso alle pda era possibile in quanto l'indirizzo *URL* era scritto in chiaro *online* e non opportunamente criptato, come sarebbe stato necessario per assicurare la riservatezza dei dati in questione.

L'Ufficio -pur senza adottare provvedimenti inibitori, considerato che il problema risultava causato involontariamente, ed era stato risolto dalla società, sicché i dati in questione non erano più disponibili *online*- ha avviato un autonomo procedimento per la contestazione della sanzione amministrativa prevista dall'art. 162, comma 2-*bis* del Codice (nota 10 aprile 2012).

Diffusione di indirizzi e numeri di telefono

Sono pervenute all'Autorità le segnalazioni di numerose persone relativamente alla diffusione su un sito web, senza consenso né possibilità di opposizione, dei propri dati personali (quali nome e cognome, indirizzo e numero di telefono), riproponendo una problematica simile ad altra affrontata nel 2011 (v. provv. 7 aprile 2011 [doc. web n. 1810351], in Relazione 2011 p. 107 e ss.).

Al riguardo per accertare chi sia il gestore del sito web è stata inviata una richiesta di cooperazione al Garante canadese (*Office of the Privacy Commissioner of* Canada), poiché, in questo caso il sito parrebbe ospitato da *server* di un *provider* canadese (nota 26 ottobre 2012).

10.2. TRATTAMENTI DA PARTE DI IMPRESE CON SEDE ALL'ESTERO

Pubblicazione *online* di profili "falsi"

A seguito di alcune segnalazioni il Garante ha avviato il monitoraggio di due fenomeni particolarmente insidiosi in rete, che spesso vedono i dati di utenti italiani illecitamente trattati da imprese con sede all'estero.

Un primo caso ha riguardato l'inserimento, sul sito di una nota *social community online,* di cd. "profili *fake*", ovvero di profili "falsi", a volte corredati da fotografie, che si riferiscono a soggetti non registrati e spesso ignari, i cui dati, in alcuni casi, provengono da altri siti di *social network*. Con riguardo al sito, il Garante si è attivato nei confronti della società che lo gestisce, insediata in Gran Bretagna, al fine di ottenere la rimozione dei falsi profili, riservandosi, comunque, in presenza di altre violazioni, di richiedere l'intervento dell'*Information Commissioner*, competente sul territorio del Regno Unito (nota 11 ottobre 2012).

Nell'altro caso, è stato segnalato che un sito raccoglie, anche ad insaputa degli interessati, dati personali, quali nominativi e fotografie, tratti da internet ed in particolare da Facebook, inserendoli nelle proprie pagine web. Risulta possibile, accedendo ad un apposito servizio, votare le foto ivi inserite indicando se una persona è o meno "stupida". La rimozione dei dati avverrebbe solo a pagamento. Dagli accertamenti svolti dall'Autorità è risultato che titolare del sito è una società con sede negli USA e che, lo stesso sito risultava ospitato da un *hosting provider* dapprima presente all'interno dell'Unione europea e poi trasferito nella Federazione Russa. Tale circostanza rende particolarmente difficile un intervento del Garante.

Richiesta di accertamenti su una società americana

Da una serie di segnalazioni pervenute nel 2012 all'Autorità da parte di utenti italiani, è emerso che una società americana, che gestisce un servizio di *couchsurfing* (ossia la messa in comunicazione di persone disponibili a scambiarsi ospitalità), ha cambiato le norme di utilizzo del portale, nonché la sua *privacy policy*, successivamente alla sua trasformazione in società commerciale.

Le nuove norme di utilizzo del sito pongono seri dubbi sulla loro conformità ai princìpi sanciti nella Direttiva n. 95/46/CE in materia di protezione dei dati personali, in particolare laddove garantiscono alla Società in questione il diritto illimitato, perpetuo, irrevocabile di disporre per qualsiasi scopo dei dati caricati dagli utenti sul sito, anche in passato, ivi comprese le e-mail inviate tramite il sistema.

Le suindicate norme prevedono inoltre che i membri della *community* accettino che i termini di utilizzo possano essere cambiati dalla società in qualunque momento senza preavviso e con effetto immediato.

Si tratta di una questione delicata, che investe anche il tema della competenza dell'Autorità riguardo a trattamenti di dati personali effettuati da soggetti stabiliti fuori dal territorio dello Stato.

Al riguardo, il Garante -associandosi all'analoga richiesta dell'Autorità federale tedesca di protezione dei dati personali- ha chiesto alla *Federal Trade Commission* di indagare sulle modalità di funzionamento del sito e di essere informato sui risultati dell'indagine e sulle misure che la Commissione intenderà adottare.

Aste *online*

Un utente di un importante sito di aste *online* ha segnalato che, diversamente dal passato, a seguito della conclusione di una transazione venivano conservati a tempo indeterminato, all'interno dei profili degli utenti accessibili da chiunque, non soltanto i relativi *feedback* e il codice numerico identificativo della transazione, ma anche la descrizione dei beni che ne sono stati oggetto.

Successivamente all'istruttoria al riguardo avviata dall'Autorità si è potuto constatare che la società ha rivisto la propria *policy*, sicché una volta scaduto il termine di 90 giorni dalla conclusione dell'asta, non sono ora più disponibili, nella sezione dedicata ai *feedback*, i dati relativi al dettaglio degli oggetti compravenduti.

Facebook

In misura superiore rispetto all'anno precedente, ma in relazione a problematiche non dissimili, nel 2012 sono pervenute segnalazioni con le quali si è lamentato il trattamento illecito dei dati personali su Facebook.

Il Garante, ha contattato il titolare del trattamento (Facebook) in un'ottica di collaborazione, sottoponendo alla società americana le problematiche pervenute.

In particolare, il Garante ha chiesto informazioni relative alla creazione, lamentata dall'interessato, di numerosi profili falsi, che Facebook ha disattivato (nota 21 gennaio 2012).

Inoltre, il Garante ha ricevuto numerose segnalazioni da parte di genitori separati i quali lamentavano che l'altro genitore avesse inserito nel proprio profilo Facebook la foto del figlio, senza richiedere il consenso del genitore segnalante. In tali ipotesi il Garante ha compiuto una valutazione in concreto caso per caso, verificando, in un'ottica di tutela del preminente interesse del minore, il tipo di immagine e il grado di apertura del profilo su cui essa era stata inserita.

11. Il trattamento di dati personali nel settore delle comunicazioni elettroniche

11.1. L'applicabilità del Codice alle persone giuridiche

Il Garante, con il provvedimento generale del 20 settembre 2012 (in G.U. 16 novembre 2012, n. 268 [doc. web n. 2094932]), volto a rispondere alle numerose istanze e richieste di chiarimenti pervenute, si è pronunciato sull'applicabilità del Codice alle persone giuridiche, enti e associazioni, a seguito della parziale abrogazione, di talune disposizioni contenute nella parte prima del Codice stesso, quali l'art. 4 relativo, tra l'altro, alle nozioni di "*interessato*" e di "*dato personale*", che fanno ora riferimento esclusivamente alle persone fisiche e non più a quelle giuridiche o assimilate (art. 40, secondo comma, del d.l. n. 201 del 6 dicembre 2011, convertito con l. n. 214 del 22 dicembre 2011 cd. "decreto salva Italia", in G.U. 6 dicembre 2011, n. 284).

L'Autorità ha chiarito che le persone giuridiche, gli enti e le associazioni continuano a non poter essere contattati se iscritti nel Registro delle opposizioni né possono ricevere, senza consenso specifico per la finalità promozionale, telefonate automatizzate con messaggi preregistrati, e-mail, fax, sms, mms aventi contenuto pubblicitario.

In effetti, le persone giuridiche, gli enti e le associazioni continuano a beneficiare delle tutele previste da alcune delle disposizioni del Codice, in particolare quelle di cui al Capo 1 ("Servizi di comunicazione elettronica") del Titolo X ("Comunicazioni elettroniche"), di diretta derivazione comunitaria poiché emanate in attuazione della Direttiva n. 2002/58/CE, e di recente integrate e modificate dal d.lgs. 28 maggio 2012, n. 69 a seguito del recepimento della Direttiva n. 2009/136/CE (in G.U. 31 maggio 2012, n. 126).

La quasi totalità di tali disposizioni è infatti rivolta a destinatari individuati non in funzione della qualifica soggettiva (persone fisiche o giuridiche), bensì quali "contraenti", termine che di recente ha sostituito nelle disposizioni del Codice quello di "abbonato" e che riguarda, a differenza di quest'ultimo, certamente anche le persone giuridiche. Diversamente interpretando, il nostro Paese rischierebbe, tra l'altro, una procedura d'infrazione comunitaria per non aver recepito nell'ordinamento nazionale le regole che a livello europeo garantiscono specifiche tutele alle persone giuridiche-contraenti.

Questa interpretazione si riferisce ad una specifica parte del Codice, ma l'impianto normativo generale, complesso e di non agevole lettura, comporta comunque per le imprese una riduzione delle forme di tutela, solo in parte risolvibile con l'esercizio dei poteri di iniziativa *ex officio* del Garante.

Ad avviso dell'Autorità è pertanto opportuna un'ulteriore valutazione di queste problematiche da parte di Governo e Parlamento, per eventuali iniziative di competenza.

11.2. LE CHIAMATE INDESIDERATE PER FINALITÀ PROMOZIONALI

Come già nel 2011 (cfr. Relazione 2011 p. 100) anche nel 2012 sono pervenute numerosissime segnalazioni riguardanti l'effettuazione di chiamate promozionali indesiderate, sia ad utenze pubblicate negli elenchi telefonici ed iscritte nel Registro delle opposizioni, sia, in misura minore ad utenze riservate, non inserite nell'elenco.

Nel 2012 è anche emersa la problematica del *telemarketing* svolto con telefonate che non consentono l'identificazione della linea chiamante (*calling line identification*), in relazione alla quale sono stati adottati tre provvedimenti di blocco del trattamento dei dati nei confronti di altrettante società (provv.ti 23 febbraio 2012 [doc. web nn. 1877065, 1877080 e 1878559], cfr. Relazione 2011 p. 101).

In termini generali gli utenti, spesso utilizzando opportunamente il modello di segnalazione pubblicato sul sito istituzionale dell'Autorità, hanno circostanziato in maniera più esaustiva le segnalazioni, con riferimento sia alle tipologie delle chiamate ricevute, sia all'indicazione dei soggetti chiamanti.

Per agevolare gli interessati è stata aggiornata la sezione "Telefonate indesiderate. Come opporsi?" del sito istituzionale dell'Autorità, inserendo un modello anche per la segnalazione di telefonate pubblicitarie indesiderate su utenze riservate.

Nell'insieme gli operatori hanno dimostrato una maggiore attenzione al rispetto della disciplina in materia, e in tal senso la Fondazione Ugo Bordoni, in qualità di gestore del Registro, ha evidenziato che nell'anno di riferimento sono sensibilmente aumentate le richieste volte a verificare l'eventuale iscrizione nel Registro stesso delle utenze da contattare.

Inoltre, il Garante ha svolto un puntuale monitoraggio delle comunicazioni che gli

operatori telefonici, in qualità di titolari del trattamento, erano tenuti ad inviare all'Autorità, con riguardo all'avvenuta adozione dei nuovi modelli di informativa e di richiesta di consenso, in base al provvedimento del 24 febbraio 2011 su "Modelli di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati ai servizi di telefonia fissa e mobile" [doc. web n. 1794638].

In questo quadro, dopo il filtro preliminare operato dall'Urp per individuare i presupposti di possibili violazioni, l'Ufficio ha avviato, spesso in relazione a ciascuna telefonata indesiderata, specifiche istruttorie preliminari.

Esse sono risultate più complesse quando i segnalanti non hanno indicato il numero chiamante (talora per l'estrema genericità delle segnalazioni, talaltra perché non tutti i cittadini dispongono dello specifico dispositivo che consente di visualizzare i numeri in ingresso).

Quando, invece, sono stati indicati i numeri chiamanti, si è potuto identificare più rapidamente chi aveva effettuato la telefonata, previa richiesta ai gestori di telefonia per conoscere la titolarità delle utenze, spesso contattate da diversi soggetti, localizzati sia in Italia sia all'estero, per conto di società committenti appartenenti a più settori economici (in particolare quello telefonico, energetico e quello connesso alla fornitura di altri servizi pubblici locali, quale il servizio idrico). Per un efficace contrasto del fenomeno sia sul territorio nazionale, sia al di fuori di esso, è stato richiesto ad una significativa parte degli operatori, non solo telefonici, di comunicare tutti i rapporti intercorrenti con società terze, nonché il numero dei *call center* o dei *partner* commerciali di cui normalmente si avvalgono.

In definitiva, l'attività di contrasto al fenomeno del *telemarketing* cd. "selvaggio" è stata anche per questo anno molto decisa ed in diversi casi sono stati aperti procedimenti sanzionatori. Sulla base degli elementi emersi in sede istruttoria, al fine di verificare la liceità del trattamento dati effettuato per finalità di *telemarketing*, sono state svolte numerose attività di carattere ispettivo (cfr. *infra* par. 20.4.).

A seguito di una complessa ed articolata attività istruttoria il Garante ha rilevato come diversi operatori telefonici effettuassero chiamate di carattere promozionale sulle utenze della propria clientela, in mancanza di un consenso adeguatamente documentato al trattamento

per finalità di *marketing* (v. art. 23 del Codice, provv. 30 maggio 2007 [doc. web n. 1412598]). Sono così state riscontrate varie violazioni della disciplina e conseguentemente avviati diversi procedimenti sanzionatori.

Tra i diversi quesiti pervenuti in argomento si segnala quello relativo al provvedimento generale del 19 gennaio 2011 recante "Prescrizioni per il trattamento di dati personali per finalità di *marketing*, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del Registro pubblico delle opposizioni" [doc. web n. 1784528] che indica entro quali limiti gli operatori del settore possono utilizzare i dati personali degli "abbonati" presenti negli elenchi telefonici per chiamate con operatore, per inviare materiale pubblicitario, o per ricerche di mercato.

È stato in particolare rappresentato che tale provvedimento, riguardando esclusivamente le attività di *telemarketing*, lascerebbe invariato l'ambito di applicazione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici e quindi l'esenzione dal consenso previsto anche ai sensi dell'art. 24 del Codice, nonché l'esenzione dall'obbligo di iscrizione al menzionato Registro pubblico delle opposizioni qualora, nell'ambito dell'attività di ricerca, si utilizzino dati tratti dagli elenchi telefonici (art. 130, comma 3-*bis*, del Codice).

L'Ufficio ha al riguardo chiarito che laddove le ricerche di mercato perseguano esclusivamente finalità di indagine statistica, scientifica e di studio, la citata specifica disciplina sul *telemarketing* e, quindi, le prescrizioni dettate dal Garante nel citato provvedimento, non trovano applicazione. Laddove, invece l'attività sia rivolta non alla mera comprensione ed analisi dei fenomeni sociali e di mercato, ma ad altre finalità che ben possono rientrare nell'attività di *marketing* (ad es., fornendo gli elementi di valutazione e selezione di nuovi segmenti e strategie di mercato per la promozione e commercializzazione di prodotti e servizi) e venga altresì effettuata mediante operatore telefonico, utilizzando i dati personali tratti da elenchi telefonici, essa va ricompresa tra quelle indicate dall'art. 7 comma 4 lett. *b),* del Codice, con la conseguente applicazione delle disposizioni del successivo art. 130 e delle specifiche prescrizioni del Garante.

11.3. LE TELEFONATE "MUTE"

Anche nel 2012, in relazione ad un numero crescente di segnalazioni, dopo l'adozione di un primo provvedimento in materia, il 6 dicembre 2011 ([doc. web n. 1857326] v. Relazione 2011 p. 104 e ss.), è proseguita l'azione di contrasto al fenomeno delle chiamate "mute", nelle quali il destinatario, dopo aver sollevato il ricevitore, non viene messo in comunicazione con alcun interlocutore.

Tali telefonate ingenerano nel chiamato particolare ansia, sospetto, fastidio, senso di impotenza, sia poiché si è naturalmente portati a porle in diretta relazione con comportamenti illeciti o delinquenziali (controlli indebiti, molestie, indagini di malintenzionati preliminari alla commissione di eventuali reati, quali furti o aggressioni), sia perché si ha la sgradevole sensazione dell'impossibilità di essere messi in contatto con qualcuno potenzialmente foriero di rilevanti informazioni. Non sono state rare, infatti, le segnalazioni nelle quali gli interessati hanno corredato di significativi particolari le loro denunce: l'avere figli adolescenti fuori di casa, genitori anziani non conviventi, familiari malati.

Dai controlli effettuati è emerso, preliminarmente, che in tutti i casi si trattava di telefonate effettuate da *call center* per finalità commerciali, mediante l'impiego di sistemi automatizzati di instradamento della chiamata agli operatori, sicché l'Autorità ha svolto diversi accertamenti di carattere ispettivo nei confronti sia delle società committenti, sia dei *call center* cui quelle attività erano state affidate, spesso in qualità di responsabili del trattamento.

Le ispezioni hanno avuto finalità conoscitive, di monitoraggio e di accertamento non solo di carattere giuridico, ma anche tecnico. Le relative istruttorie sono in via di definizione.

11.4. DATI TRATTI DA INSERTI PUBBLICITARI

Negli anni 2011 e 2012 sono pervenute numerose segnalazioni relative a telefonate promozionali indesiderate aventi ad oggetto vari prodotti alimentari di una società, destinataria di un provvedimento inibitorio e prescrittivo del 3 dicembre 2009 [doc. web n. 1679436]. Dall'istruttoria è risultato che l'attività di *telemarketing* veniva effettuata da una nuova società, subentrata anche nel *database* dei clienti della società inibita -nel frattempo fallita- successivamente implementato fino a comprendere un milione di soggetti.

Inoltre, tale nuova società acquisiva anche direttamente i dati personali degli interessati tramite svariate modalità (ad es., inserti pubblicitari su riviste; moduli cd. "presenta amico", posta elettronica) e svolgeva attività di *telemarketing*, avvalendosi di alcuni *call center*, anche verso soggetti che si erano limitati a manifestare interesse per la sua attività, senza averne preventivamente acquisito il necessario specifico consenso.

Oltre a vietare l'ulteriore trattamento dei dati personali per le attività diverse da quelle contrattuali, l'Autorità ha prescritto alla società sia di fornire a tutti i clienti l'informativa con gli ulteriori elementi richiesti dall'art. 13 del Codice, sia di richiedere agli interessati il preventivo consenso al trattamento dei dati personali libero, informato, documentato per iscritto e specifico per ogni diversa finalità del trattamento ed in particolare per l'invio di proposte commerciali e per la comunicazione dei dati personali a soggetti terzi; ha prescritto altresì di utilizzare i dati tratti da elenchi telefonici previo il necessario riscontro presso il Registro pubblico delle opposizioni (provv. 11 ottobre 2012 [doc. web n. 2089777]).

11.5. INTERCETTAZIONI PER INDAGINI DI CARATTERE PENALE

Nel 2005 il Garante all'esito di un'istruttoria svolta nei confronti dei principali fornitori di servizi telefonici e telematici e riguardante le modalità con cui essi adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni aveva prescritto ai medesimi fornitori l'adozione di alcune misure e di specifici accorgimenti volti a incrementare, sotto ogni profilo, il livello di sicurezza dei dati personali trattati nell'ambito delle attività di intercettazione, soprattutto per quanto riguarda i rapporti tra i fornitori e l'autorità giudiziaria (v. provv. 15 dicembre 2005 [doc. web n. 1203890]).

Nel settembre 2012 è stata avviata una nuova attività istruttoria nei confronti dei principali fornitori, mediante la richiesta di elementi conoscitivi volti a verificare, da un lato, l'attualità delle misure e degli accorgimenti prescritti in passato e, dall'altro, l'eventuale predisposizione, da parte degli stessi, di nuove e più avanzate misure di sicurezza. Analogamente, il Garante ha rivolto la sua attenzione anche agli uffici giudiziari, tramite una parallela attività istruttoria (cfr. *supra* par. 4.9.).

11.6. DATI UTILIZZATI A FINI DI PROFILAZIONE

Con riguardo ai trattamenti di profilazione svolti dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, attraverso i dati personali aggregati della propria clientela, senza l'acquisizione del necessario consenso (v. provv. generale 25 giugno 2009 [v. doc. web n. 1629107]), il Garante ha emanato una serie di provvedimenti di blocco impedendo l'uso dei dati raccolti. Ciò sino alla verifica della completa e puntuale attuazione di tutte le misure tecnico-giuridiche prescritte con i diversi provvedimenti emanati a seguito delle specifiche istanze di *prior checking* presentate all'Autorità dalle singole compagnie telefoniche, (cfr. Relazione 2011 p. 114) .

Rispetto all'attività di profilazione, il Garante ha altresì esaminato tutte le nuove istanze di verifica preliminare presentate nel 2012 dagli operatori telefonici. In tale ambito sono stati emanati nuovi provvedimenti volti a consentire agli operatori l'utilizzo di dati aggregati degli utenti per finalità di profilazione avvalendosi dell'esonero dall'acquisizione del relativo consenso, previa attuazione delle diverse prescrizioni dell'Autorità.

In particolare, in uno specifico caso il Garante ha consentito ad una società telefonica, previa adozione di una serie di articolate misure di sicurezza, un nuovo trattamento di arricchimento del *database* clienti, attraverso l'incrocio dei dati aggregati di traffico degli utenti con altre categorie di dati personali ed informazioni di natura prevalentemente statistica, tratte da fonti esterne alla società istante. Ciò per favorire ulteriori prospettive di servizi ed offerte nello specifico campo della telefonia, attraverso la creazione di nuovi e più ricchi *cluster* di utenza, assicurando però al contempo il corretto trattamento dei dati personali e un adeguato livello di tutela dei diritti e delle libertà fondamentali degli interessati.

11.7. RICEVITORIE E TABACCHERIE

Nel 2012 l'Autorità ha completato un ciclo di accertamenti ispettivi avviati dal mese di ottobre 2011, volti a 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, che in materia ha adottato già un provvedimento il 15 dicembre 2011 [doc. web n. 1883880] inibitorio e prescrittivo nei confronti di una nota società operante nel settore dei giochi e servizi resi tramite ricevitorie, ha monitorato il trattamento dati effettuato da alcune società afferenti ad un altro noto gruppo del medesimo settore. Al riguardo, pur non essendo stati ravvisati i presupposti per l'adozione di un provvedimento del Collegio, è emerso che le dette società, prima dell'adozione di nuovi contratti-tipo, utilizzavano, in contrasto con l'art. 23 del Codice, una formula di consenso unico al trattamento dei dati personali dei punti vendita per la finalità contrattuale e per quella promozionale e si limitavano ad avvisare punti vendita e ricevitorie che "*il conferimento dei dati era necessario*", senza alcuna distinzione per tipologia di dati o finalità perseguita.

Inoltre, è risultato che le società in questione avevano effettuato campagne di incentivazione per la vendita dei propri servizi nei confronti dei punti vendita, senza il necessario consenso distinto e specifico. Pertanto l'Ufficio ha avviato un procedimento sanzionatorio nei confronti di tutte le società del gruppo coinvolte in tale trattamento dati (nota 20 luglio 2012).

11.8. CESSIONI DI DATI PERSONALI A FINI DI *TELEMARKETING*

Con provvedimento del 5 aprile 2012 [doc. web n. 1891156], il Garante ha ribadito che l'acquirente di liste di dati personali da utilizzare per attività di *telemarketing* deve verificare che gli interessati abbiano espresso il proprio preventivo consenso ai contatti di natura commerciale. Il caso riguardava un interessato i cui dati erano stati tratti da un questionario *online* che, a seguito degli accertamenti effettuati dall'Autorità, non è risultato conforme alla disciplina di legge, dal momento che prevedeva come obbligatoria la prestazione del consenso dell'interessato a fini promozionali (v. art. 23 del Codice).

Nel contratto di fornitura delle liste dei potenziali clienti, inoltre, i rapporti tra le parti erano regolati in modo da ricondurre la formale qualifica di titolare del trattamento alla sola società fornitrice dei dati personali degli interessati, nonostante diverse pattuizioni evidenziassero un ruolo sostanziale di titolare anche della società acquirente i dati, potendo questa determinare le finalità e modalità dei contatti promozionali effettuati per proprio conto e nel proprio interesse.

Per queste ragioni, il Garante ha ritenuto che anche l'acquirente dovesse essere considerato titolare dell'attività di *telemarketing* in questione, ed ha dichiarato illecito e vietato il trattamento effettuato in assenza del prescritto consenso dei singoli interessati al trattamento per finalità promozionali (provv. 5 aprile 2012 [doc. web n. 1891156].

11.9. *MOBILE PAYMENT*

Nel 2012 in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, noti come *mobile remote payment* e *mobile proximity payment,* l'Autorità ha acquisito presso i diversi soggetti interessati (oltre agli operatori telefonici, gli istituti bancari, i circuiti delle carte di credito, i *merchant* ed i cd. "*hub* tecnologici"), una serie di informazioni. In particolare, con riguardo ai servizi che consentono di attivare "in remoto" il pagamento di un bene o di un servizio, l'Autorità ha analizzato i sistemi e le modalità con le quali gli operatori telefonici, gli *hub* tecnologici incaricati della gestione tecnica del servizio e diversi *merchant,* consentono ai propri clienti di effettuare micropagamenti per l'acquisito di servizi e prodotti digitali fruibili tramite *smartphone*, PC e *tablet*, con conseguente addebito del relativo costo sul conto telefonico dell'utente, o attraverso decurtazione dell'importo dal credito telefonico nel caso di carte ricaricabili.

Con riguardo, invece, ai servizi che includono pagamenti elettronici di "prossimità", per i quali è necessaria una vicinanza fisica tra il dispositivo mobile ed il prodotto o servizio acquistato (attraverso il ricorso alla tecnologia *NFC* (*Near Field Communication*), il Garante ha svolto la suddetta attività anche presso alcuni istituti bancari ed alcuni dei circuiti delle carte di credito.

Le indagini dell'Autorità sono state estese anche ad un noto motore di ricerca.

Questa attività conoscitiva costituisce la base per predisporre una regolamentazione di tali servizi che consenta, favorendo l'uso delle descritte tecnologie, un utilizzo corretto dei dati personali degli utenti da parte dei soggetti coinvolti.

11.10. LA DISCIPLINA DEI *DATA BREACH*

In attuazione della direttiva comunitaria in materia di sicurezza e *privacy* nel settore delle comunicazioni elettroniche (Direttiva n. 2009/136/CE, di recente recepita con il d.lgs. 28

maggio 2012, n. 69, in G.U. 31 maggio 2012, n. 126), il nuovo art. 32-*bis* del Codice prevede che i fornitori di servizi di comunicazione elettronica accessibili al pubblico (quali telefonia, accesso a internet, *account* di posta elettronica) sono obbligati a comunicare senza indebiti ritardi al Garante e, in alcuni casi, al contraente o ad altre persone interessate, il verificarsi di eventi, qualificati come "*violazioni di dati personali*", riguardanti i dati personali contenuti nei *database* di tali soggetti.

Alla base di tale normativa vi è la consapevolezza che un evento che coinvolga i dati personali trattati dai suindicati soggetti, se non gestito in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente (o alle altre persone interessate), tra cui l'usurpazione d'identità (cfr. considerando 61, Direttiva n. 2009/136/CE).

Al riguardo, il 26 luglio 2012 il Garante ha adottato le "Linee-guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (in G.U. 7 agosto 2012, n. 183 [doc. web n. 1915485]) recanti prescrizioni nei confronti dei fornitori, con particolare riguardo: all'individuazione dei soggetti tenuti a comunicare la violazione; alle circostanze in cui la comunicazione dev'essere effettuata; all'obbligo di avvisare anche gli utenti; alle misure di sicurezza tecniche e organizzative da adottare.

In sostanza, è stato chiarito che l'obbligo di comunicare i *data breach* spetta esclusivamente ai fornitori di servizi telefonici e di accesso a internet, non riguardando viceversa le reti aziendali, gli internet *point* (che si limitano a mettere a disposizione dei clienti i terminali per la navigazione), i motori di ricerca, i siti internet che diffondono contenuti.

La comunicazione, anche sommaria, deve avvenire entro ventiquattro ore dalla scoperta dell'evento: i fornitori devono dare le informazioni utili ad una prima valutazione dell'entità della violazione ed hanno tre giorni di tempo per una descrizione più dettagliata. All'esito delle verifiche, i medesimi soggetti devono comunicare al Garante le modalità con le quali hanno posto rimedio alla violazione e le misure adottate per prevenirne di nuove. Al fine di agevolare l'adempimento, il Garante ha predisposto anche un modello di comunicazione, disponibile *online* in formato pdf [doc. web n. 1915835].

Nei casi più gravi, i fornitori hanno l'obbligo di informare anche gli interessati considerando, tra l'altro, il pregiudizio che la perdita, la distruzione o l'accesso non

autorizzato ai dati può comportare (furto di identità, danno fisico, danno alla reputazione), l'"attualità" dei dati (dati più recenti possono rivelarsi più interessanti per i malintenzionati), e la loro qualità (finanziari, sanitari, giudiziari).

Con la citata delibera 26 luglio 2012 è stata contestualmente avviata una consultazione pubblica per acquisire osservazioni in merito ad alcune, specifiche modalità applicative della nuova disciplina, contenuta nell'art. 32-*bis* del Codice.

Dal 1° giugno 2012, data di entrata in vigore della disciplina in materia di *data breach*, sono pervenute all'Autorità diverse comunicazioni di violazioni, da parte di fornitori di servizi di comunicazione elettronica di grandi dimensioni.

Nei casi la cui trattazione è stata conclusa, l'Autorità ha verificato che fossero state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe e non ha ritenuto necessario adottare provvedimenti specifici.

Relativamente ad altre comunicazioni di *data breach* gli accertamenti sono ancora in corso.

11.11. L'UTILIZZO DEI *COOKIE*. *FAQ*

La disciplina relativa all'uso dei cd. *"cookie"* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente) e degli altri strumenti analoghi (quali web *beacon/web bug, clear GIF*) è stata modificata, a seguito dell'attuazione della Direttiva n. 2009/136/CE (che è intervenuta sulla Direttiva n. 2002/58/CE, la cd. "Direttiva *e-Privacy*"), ad opera del d.lgs 28 maggio 2012, n. 69.

In sostanza, il nuovo art. 122 del Codice consente l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate a condizione che tali soggetti abbiano espresso il proprio consenso sulla base di un'informativa semplificata (art. 13, comma 3, del Codice). La disciplina dei *cookie* si basa pertanto sul principio del cd. "*opt-in*", eccezion fatta per i dispositivi di natura tecnica, ossia quelli strettamente necessari ad effettuare la trasmissione della comunicazione o alla fornitura del servizio esplicitamente richiesto dall'abbonato o dall'utente. Per questi ultimi, la legge prevede ora il libero utilizzo, ferma restando la necessità che contraenti e utenti vengano sempre adeguatamente informati.

Al riguardo, il Garante ha avviato una consultazione pubblica volta a individuare le modalità semplificate per l'informativa di cui all'art. 13, comma 3, del Codice, da rendere *online* sull'utilizzo dei suindicati dispositivi (provv. 22 novembre 2012, in G.U. 19 dicembre 2012, n. 295 [doc. web n. 2139697]).

Al fine di fornire comunque prime indicazioni sul tema il 18 dicembre 2012 l'Autorità ha anche pubblicato sul proprio sito internet apposite *FAQ* [doc. web n. 2142939].

11.12. LA LOTTA ALLO *SPAM*

Anche nel 2012 il Garante ha ricevuto numerose richieste d'intervento relative ad attività di *spam* realizzata mediante diversi mezzi (posta elettronica, fax, chiamate telefoniche preregistrate, sms); rispetto agli anni precedenti, appaiono diminuite le segnalazioni riguardanti fax indesiderati, anche in ragione dei numerosi provvedimenti inibitori e prescrittivi adottati dall'Autorità, che hanno in taluni casi comportato l'applicazione di sanzioni amministrative di notevole importo.

Fax e e-mail risultano comunque più utilizzati per le attività di *spam* rispetto agli sms.

In un'occasione, l'Autorità, considerato il numero degli interessati e le affermazioni rese dal titolare riguardo alle modalità del trattamento dati, ha adottato un provvedimento inibitorio e prescrittivo (provv. 21 marzo 2012 [doc. web n. 1895176]), di seguito sintetizzato, ed avviato autonomi procedimenti sanzionatori per la contestazione delle sanzioni amministrative previste dagli artt. 161 e 162, comma 2-*bis,* del Codice (note 27 febbraio, 27 e 31 agosto 2012).

Più spesso, quando l'invio di comunicazioni promozionali automatizzate è risultato occasionale, oppure frutto di un mero errore, l'Autorità ha inviato ai titolari del trattamento apposite note di richiamo al pieno rispetto della disciplina in materia (*ex multis* nota 24 maggio 2012).

Anche in materia di *spam* rileva la questione dell'applicabilità del Codice alle persone giuridiche ed agli enti assimilati, poiché il decreto "salva Italia" (d.l. n. 201/2011 convertito con l. 22 dicembre 2011 n. 214) ora include nel concetto di "interessato" di cui all'art. 4 del Codice le sole persone fisiche (v. *supra* par. 2.1.1.).

Fax indesiderati

Il 21 marzo 2012 l'Autorità ha adottato un provvedimento inibitorio e prescrittivo nei confronti di una società italiana svolgente attività di *tour operator* appartenente ad un gruppo spagnolo [doc. web n. 1895176], la quale aveva inviato comunicazioni promozionali indesiderate via fax, talora nonostante l'interessato avesse comunicato più volte alla medesima società il diniego al trattamento dei propri dati personali. Il Garante ha vietato il trattamento dati in essere, prescrivendo altresì di rilasciare un'idonea informativa e di acquisire il consenso degli interessati, specifico, espresso e documentato per iscritto, da ottenere anche qualora i dati siano tratti da elenchi pubblici o da siti web (cfr. provv. 14 luglio 2005 [doc. web n. 1151640] e provv. 2 marzo 2011 [doc. web n. 1802423]).

Invio di fax per l'iscrizione in banche dati a pagamento

Un'associazione, che a sua volta aveva raccolto le lamentele di varie imprese, ha segnalato l'invio a vari destinatari di moduli contrattuali con i quali una società insediata in Slovacchia, affermando di gestire un cd. "registro del mercato nazionale" invitava i destinatari, iscritti a loro insaputa nel registro stesso, a confermare l'esattezza dei dati riportati sui moduli inviati o a fornire quelli corretti.

L'attività è apparsa, in particolare, in possibile contrasto con gli obblighi in materia di informativa e consenso per il trattamento di dati personali, relativi all'invio di comunicazioni promozionali (v. artt. 13 e 23 del Codice). Pertanto, il Garante ha avviato un'apposita cooperazione con l'Autorità slovacca, le cui verifiche hanno evidenziato che i dati erano stati tratti da fonte pubbliche e i destinatari iscritti nel registro *de quo* a loro insaputa.

L'Autorità slovacca ha pertanto impartito precise prescrizioni alla società, con particolare riferimento all'obbligo di rilasciare ai soggetti iscritti nel registro un'informativa idonea indicante i tipi di dati trattati, la loro origine e la possibilità di decidere riguardo al trattamento dati, specialmente quando quest'ultimo sia associato ad eventuali pagamenti.

Mail Spamming

Rimangono numerose le violazioni via e-mail, per le quali talvolta risulta difficile individuare i titolari del trattamento, 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 *extra*-europei, ove l'Autorità non ha competenza (art. 5 del Codice).

In diversi casi, invece a seguito di istruttorie talvolta anche complesse, L'Autorità ha

verificato che l'invio di fax e, ancor più di e-mail, promozionali indesiderati è stato effettuato da società localizzate in Paesi europei (in particolare, Francia, Svizzera, Regno Unito) ed ha richiesto la collaborazione delle Autorità dei rispettivi Paesi per far cessare gli invii indesiderati.

Talora, queste Autorità hanno richiesto chiarimenti direttamente alle società mittenti, invitandole al rispetto dei diritti degli interessati, sanciti, pur con qualche peculiarità, anche dai rispettivi ordinamenti (nota 19 settembre 2012).

Va però considerato 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 alla tutela e ai rimedi azionabili.

In un particolare caso, l'accertamento relativo all'invio di alcune e-mail indesiderate è stata l'occasione per l'adozione di un provvedimento inibitorio e prescrittivo in materia di acquisizione di dati personali *online* per finalità eterogenee (provv. 20 dicembre 2012 [doc. web n. 2223607]). In tale occasione, coerentemente con l'ottica semplificatoria prevalente nella più recente legislazione nazionale, il Garante -oltre a inibire il trattamento dati posto in essere e a dare apposite prescrizioni- ha ricordato, tuttavia, l'eccezione del cd. "*soft spam*", in base al quale, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso (v. art. 130, comma 4).

Da alcune segnalazioni è emerso che chiunque, accedendo al sito di una nota compagnia di assicurazioni, poteva richiedere preventivi Rca inserendo indirizzi di posta elettronica di altri soggetti ad insaputa di questi ultimi e della stessa compagnia assicuratrice. Il fenomeno ha comportato l'invio massivo ed incontrollato, sulle caselle di posta elettronica di ignari soggetti, di e-mail contenenti preventivi mai richiesti.

Al fine di arginare tale fenomeno l'Autorità, dopo una ampia ed articolata attività istruttoria, da un lato ha verificato l'adozione di misure organizzative e tecniche volte ad

impedire che soggetti ignoti anche alla stessa compagnia, continuassero a sollecitare preventivi non richiesti dagli interessati, dall'altro ha dettato ulteriori accorgimenti a tutela dei dati personali degli ignari titolari di indirizzi di posta elettronica.

In particolare le misure di sicurezza adottate dalla compagnia assicuratrice hanno riguardato:

1) l'attivazione di un apposito elenco di esclusione che consente di bloccare l'invio di e-mail ad utenti che abbiano già lamentato la ricezione di comunicazioni indesiderate;

2) la previsione di un sistema automatizzato di *alert* (nello specifico l'invio di una e-mail di avvertenza) qualora la richiesta di invio di preventivi al medesimo indirizzo di posta elettronica superi una determina soglia nell'arco di una giornata.

A tali misure si è aggiunta la specifica indicazione dell'Autorità di contrassegnare l'e-mail di avvertenza con caratteri, anche grafici, di chiarezza ed immediatezza tali da consentire all'utente sia di distinguerla da altre e-mail ricevute, sia di fornire un più semplice riscontro.

Dopo questi interventi non risultano all'Autorità, ulteriori segnalazioni in merito.

11.13. L'ISTRUTTORIA RELATIVA AD UN SERVIZIO DI TELEFONIA *IP* (INTERNET *PROTOCOL*)

Un utente dei servizi di messaggistica, condivisione *file* e comunicazione vocale offerti dalla società Skype S.a.r.l. ha lamentato l'impossibilità di eliminare definitivamente il proprio *account*.

Come verificato dall'Autorità, le indicazioni contenute nella guida *online* disponibile sul sito internet della società, alla sezione *FAQ*, chiariscono in effetti che "*una volta creato, non è possibile eliminare un account Skype o cambiare un nome Skype. Tuttavia, puoi rimuovere tutti i dati personali contenuti nel tuo profilo*"; con l'avvertenza che, a seguito di tale operazione, "*sarà ancora possibile cercarti tramite il tuo nome Skype*".

Alla richiesta di cancellazione rivoltale dal segnalante la società aveva replicato, invece, che tale operazione è possibile, ma che per consentire una puntuale verifica circa l'identità del richiedente, questi deve indicare mese ed anno di creazione del proprio *account*. Tale adempimento era stato ritenuto dal segnalante troppo oneroso, trattandosi di *account* creato molto tempo prima ed in relazione al quale non aveva tale memoria di dettaglio.

La società, pur sottolineando di essere soggetta alla normativa lussemburghese in materia di protezione dei dati personali (oltre che, ovviamente, alle previsioni della Direttiva n. 95/46/CE) e riconoscendo, pertanto, la competenza esclusiva dell'Autorità Garante del Lussemburgo, ha comunque rappresentato che:

1) le procedure per la verifica dell'identità di chi chiede la cancellazione del proprio *account* sono adottate per minimizzare il rischio che l'istanza provenga da soggetti non autorizzati ovvero abbia carattere fraudolento; inoltre, Skype ha dichiarato di detenere una quantità minima di dati per poter associare un determinato soggetto ad uno specifico *account*, specie se quest'ultimo è gratuito. Né, al riguardo, i documenti di identità sarebbero idonei a comprovare con certezza la riconducibilità di quella persona all'*account* in questione;

2) con riferimento alle *FAQ* del proprio sito, Skype, a seguito dell'intervento dell'Autorità, si è ripromessa di aggiornarle ed eventualmente modificare le procedure atte a consentire agli utenti di chiudere, in autonomia, il proprio *account*. In realtà, le procedure adottabili in modo autonomo dagli utenti possono portare non alla chiusura dell'*account*, ma solo alla cancellazione di una o più delle informazioni presenti sul profilo dell'utente (quali il nome utente o *username*, i dati anagrafici, l'indirizzo e-mail, il numero di telefono). In tale evenienza, lo *username* comunque rimarrebbe, in modo che altri utenti che già ne fossero a conoscenza, sarebbero comunque in grado di contattare quello specifico utente;

3) Skype ha riconosciuto che le *FAQ*, allo stato, non chiariscono che il servizio di supporto tecnico clienti può bloccare permanentemente (non dunque cancellare) l'*account*, rimuovendo lo *username* dalle *directories* pubbliche, in modo che non sia più visibile dagli altri utenti, con la medesima procedura prevista in caso di frodi o abusi.

L'*username* resta in tal caso archiviato dai sistemi della società, per evitare che in futuro altri soggetti possano utilizzare il medesimo nome e indurre confusione negli utenti del servizio. Anche in questa ipotesi, l'utente può comunque rimuovere le proprie informazioni personali dal profilo prima che l'*account* sia bloccato.

Questi chiarimenti hanno evidenziato che, a fronte di una richiesta di cancellazione, Skype si limita in realtà a fornire un servizio di mera deindicizzazione continuando a detenere alcuni dati personali degli utenti.

Permane pertanto la necessità di verificare la tipologia dei dati conservati dopo la chiusura dell'*account*, i tempi e le modalità di tale conservazione, della quale peraltro l'utente potrebbe non essere ben informato.

Per tali motivi, il Garante ha deciso di avviare ulteriori approfondimenti e, data la rilevanza del fenomeno (Skype conta milioni di utenti in tutto il mondo), di ampliare il contesto di riferimento, sottoponendo la tematica all'esame del Gruppo di lavoro *ex* Art. 29.

12. La propaganda elettorale e le associazioni

In prossimità delle consultazioni elettorali amministrative del 2012 e politiche del 2013, l'Autorità ha approvato due provvedimenti che confermano le regole già stabilite in materia dal provvedimento generale del 7 settembre 2005 ([doc. web n. 1165613], in G.U. 12 settembre 2005, n. 212 Relazione 2005 p. 65), prevedendo speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati ed individuando le corrette modalità in base alle quali tali soggetti possono utilizzare a fini di propaganda elettorale i dati personali dei cittadini (es. indirizzo, telefono, e-mail) (provv. 5 aprile 2012 [doc. web n. 1885765], in G.U. 16 aprile 2012, n. 89 e provv. 10 gennaio 2013, in G.U. 14 gennaio 2013, n.11 [doc. web n. 2181429]).

È stato in particolare evidenziato che per contattare gli elettori ed inviare materiale di propaganda possono essere usati, senza il consenso degli interessati, i dati contenuti nelle liste elettorali detenute dai comuni, ovvero nell'elenco degli elettori italiani residenti all'estero, in altre fonti documentali detenute da soggetti pubblici accessibili a chiunque, nonché i dati personali di aderenti ed iscritti e quelli raccolti nel quadro delle relazioni interpersonali avute con cittadini ed elettori.

È invece necessario il consenso qualora si utilizzino dati presenti sul web per altre finalità, ovvero per particolari modalità di comunicazione elettronica quali sms, e-mail, mms, telefonate preregistrate e fax.

Il consenso è altresì obbligatorio per usare sia i dati degli abbonati presenti negli elenchi telefonici, sia i dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative politiche (ad es., *referendum*, proposte di legge, raccolte di firme).

Non sono invece in alcun modo utilizzabili gli archivi dello stato civile, l'Anagrafe dei residenti, indirizzi raccolti per svolgere attività e compiti istituzionali dei soggetti pubblici o per prestazioni di servizi, anche di cura, liste elettorali di sezione già utilizzate nei seggi, dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista durante operazioni elettorali.

I soggetti che utilizzano i dati per esclusivi fini di selezione di candidati alle elezioni, di propaganda elettorale e di connessa comunicazione politica, vengono esonerati dall'obbligo

di rendere l'informativa, sino alle date indicate nei suddetti provvedimenti, solo nelle ipotesi in cui i dati stessi siano raccolti direttamente dalle predette fonti, oppure il materiale propagandistico sia di dimensioni così ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non sia possibile inserirvi un'idonea informativa, anche sintetica. Decorso il termine indicato, partiti, movimenti politici, sostenitori e singoli candidati possono continuare a trattare (anche mediante mera conservazione) i dati personali raccolti lecitamente solo informando gli interessati entro il termine indicato nei provvedimenti, nei modi previsti dall'art. 13 del Codice.

Presenta, invece, caratteri di novità il caso postosi nell'ambito delle consultazioni tenutesi in data 25 novembre e 2 dicembre 2012 per l'individuazione del candidato della coalizione di centro-sinistra alla Presidenza del Consiglio dei ministri (cd. "primarie"). Al riguardo l'Autorità (provv. 31 ottobre 2012 [doc. web n. 2079275]) ha esaminato alcuni profili problematici sollevati da un comitato e da alcuni privati cittadini in merito al trattamento dei dati personali dei partecipanti alle operazioni di voto. Tali perplessità traevano origine da alcune disposizioni del relativo regolamento, che prevedeva la necessaria sottoscrizione di un "pubblico appello" e l'iscrizione in un apposito "albo" ai fini della partecipazione alle consultazioni, con connessa possibile diffusione dei dati personali, anche sensibili, degli interessati.

Il Garante, richiamata la natura "sensibile" dei dati trattati e il connesso regime normativo, ha ribadito la necessità di attenersi ai princìpi posti dagli artt. 3 e 11 del Codice, invitando altresì il Comitato della Coalizione (nella dichiarata veste di titolare del trattamento) a stabilire modalità idonee ad evitare forme di diffusione dei dati e ad adottare adeguate misure di sicurezza a tutela dei medesimi. L'Autorità, infine, ha evidenziato la necessità di rendere un'idonea informativa preventiva agli interessati, rinviando, per la disciplina degli ulteriori profili non espressamente considerati, alle disposizioni dell'autorizzazione generale n. 3/2011.

13. La protezione dei dati personali e il rapporto di lavoro pubblico e privato

Il trattamento di dati personali riferiti a lavoratori, operanti sia nel settore pubblico che privato, continua a interessare le aree già individuate nella precedente edizione (e di seguito menzionate), nelle quali è costantemente richiesto l'intervento dell'Autorità, anche di natura ispettiva (v. *infra* par. 20.).

Segnalazioni e reclami hanno evidenziato profili in parte già trattati in passato (in particolare nel provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. web n. 1364099], e nel provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. web n. 1417809]), con riguardo alle modalità di consegna della documentazione indirizzata al singolo lavoratore (contenente, ad es., contestazioni disciplinari, notizie di carattere valutativo o sanitario), ma pure innovativi, quali la corretta configurazione del protocollo informatico e il conseguente regime (o, semplicemente, la possibilità) di accesso alle informazioni inerenti i singoli lavoratori da parte di altri colleghi.

L'utilizzo delle tecnologie "vecchie" (anzitutto i sistemi di videosorveglianza) e "nuove" (ad es., la geolocalizzazione dei veicoli aziendali e, quindi, indirettamente, dei lavoratori che ne fanno uso) continua a rappresentare una delle principali aree di intervento dell'Autorità.

Diverse segnalazioni, connesse al regime di pubblicità di documenti ed informazioni relativi ai dipendenti pubblici -in larga misura già affrontate nelle menzionate linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico nonché nelle linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011 [doc. web n. 1793203]- continuano a pervenire all'Autorità ed evidenziano carenze nella puntuale applicazione della disciplina di settore.

A seguito della promulgazione della l. 6 novembre 2012, n. 190 (Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione)

-che solo in parte ha tenuto in considerazione il contenuto della segnalazione al Parlamento e al Governo ai sensi dell'art. 154, comma 1, lett. *f)*, del Codice da parte dell'Autorità (cfr. segnalazione 10 dicembre 2009 [doc. web n. 1693019])- e considerando i quesiti e le richieste che continuano a pervenire, in particolare da parte di società (di regola multinazionali), concernenti le modalità del trattamento di dati personali in relazione alle procedure di segnalazione interna (cd. "*whistleblowing*"), il Garante ha avviato nuovi approfondimenti in materia.

Merita infine segnalare che, senza significative variazioni, è stata rinnovata l'autorizzazione generale n. 1/2012 per il trattamento dei dati sensibili nell'ambito del rapporto di lavoro (provv. 13 dicembre 2012 [doc. web n. 2158817]).

13.1. "CIRCOLAZIONE" DI INFORMAZIONI ALL'INTERNO DEL CONTESTO LAVORATIVO

Numerose sono le segnalazioni e i reclami che lamentano, all'interno del contesto lavorativo, illeciti trattamenti di dati personali ed in particolare informazioni personali rese note ad altri lavoratori (per lo più colleghi) che non ne avrebbero titolo. La fattispecie più segnalata è quella relativa alle modalità di consegna di comunicazioni individuali destinate al lavoratore (aventi il più vario contenuto) cui, con l'introduzione di sistemi di protocollazione elettronica, si sono aggiunte segnalazioni relative alla impropria configurazione di tali sistemi (che consentirebbe l'indebita acquisizione di informazione da parte di colleghi).

Notifica a mano di determinazioni

In più di una circostanza l'Autorità è stata chiamata a pronunciarsi in relazione alla notifica a mano del lavoratore di comunicazioni contenenti dati personali: tali sono stati considerati anche i dati numerici, riassunti in *report* ed elaborati al fine di monitorare l'andamento produttivo di unità organizzative.

È stato in particolare affermato, conformemente a quanto valutato in termini generali dal Gruppo Art. 29 nel Parere n. 4/2007 - WP 136, adottato il 20 giugno 2007, che i dati quantitativi e qualitativi riferiti allo svolgimento dell'attività professionale di un'unità organizzativa di un istituto previdenziale rientrano nell'ampia nozione di dato personale di cui all'art. 4 comma 1, lett. *b*) del Codice, ma non in quello di dato sensibile (provv. 18 ottobre 2012 [doc. web n. 2174351]).

Nel caso di specie, tuttavia, l'Autorità non ha ritenuto violata la disciplina sulla protezione dei dati personali in quanto la consegna nelle mani della reclamante di alcune note dirigenziali contenenti i dati in parola è risultata essere effettuata legittimamente da un'incaricata alla segreteria della dirigente firmataria delle medesime note. È stato infatti accertato, che tra i compiti degli incaricati di segreteria, uno specifico ordine di servizio prevedeva espressamente le attività oggetto di reclamo.

Ove, invece, il personale incaricato non solo della consegna, ma anche di operazioni di trattamento che comportano la conoscenza del contenuto degli atti in parola dovesse "*spillare*" o consegnare "*in busta chiusa*" un documento di cui, in ragione delle mansioni svolte, può legittimamente aver preso conoscenza, si determinerebbe un ingiustificato aggravio di adempimenti in capo al titolare del trattamento.

L'opportunità di siffatte misure è stata invece ribadita nel diverso caso in cui -con particolare riguardo al trattamento di dati sensibili- il titolare si avvalga di personale incaricato del solo recapito (si pensi, ad esempio, ai commessi; cfr. in tal senso, le indicazioni, richiamate anche nel reclamo, fornite in termini generali dal Garante al punto 5.3. delle linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, cit.; non diversamente il punto 5.5. della deliberazione 23 novembre 2006 [doc. web n. 1364939], linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati).

Il Garante ha altresì posto a fondamento della propria decisione il fatto che, anche in relazione alla consegna di documentazione contenente informazioni particolari (e comunque non sensibili) -qual è il caso delle contestazioni disciplinari- l'ordinamento ammette la consegna "*a mano*" del primo atto del procedimento disciplinare contenente la contestazione degli addebiti (cfr. art. 55-*bis*, comma 5, d.lgs. n. 165/2001), contemperando così l'esigenza di speditezza del procedimento e di certezza in capo al datore di lavoro quanto all'avvenuta notificazione della comunicazione all'interessato con la necessità di assicurare la riservatezza del lavoratore. Più in generale, peraltro, il titolare del trattamento può avere un legittimo interesse, specie in relazione a particolari tipologie di atti (ad es., atti

per i quali è stabilito un termine o dalla cui ricezione decorrono particolari effetti), ad acquisire prova dell'avvenuta ricezione degli stessi, che ben può essere precostituita salva l'adozione delle menzionate cautele nell'individuazione dell'incaricato mediante l'apposizione di una sottoscrizione ad opera del destinatario su copia della comunicazione allo stesso diretta (cfr., con riguardo, ad es., alle modalità di consegna di atti contenenti contestazioni disciplinari ovvero dell'atto di recesso, Cass. civ., sez. lav., 1 giugno 1988, n. 3716, e Cass. civ., sez. lav., 4 febbraio 1997, n. 1024).

Analoghe considerazioni sono state svolte in una fattispecie similare (provv. 18 ottobre 2012 [doc. web n. 2174582]), concernente la notifica di determinazioni aventi ad oggetto l'irrogazione di sanzioni disciplinari ad un lavoratore da parte del proprio superiore gerarchico (ancorché *ad interim*).

Protocollo informatico

Come anticipato, il Garante ha chiarito che l'accesso alle informazioni relative ai dipendenti acquisite nel protocollo informatico -il sistema informativo in cui si registrano i documenti in entrata e in uscita di un'azienda o di una pubblica amministrazione- deve essere limitato al solo personale specificamente incaricato di tali trattamenti e non può essere consentito alla generalità indifferenziata degli utenti dei servizi di protocollazione (provv. 11 ottobre 2012 [doc. web n. 2097560]). Nella vicenda oggetto di segnalazione è emerso invece che, presso un'importante sede periferica di un ente pubblico, un ampio numero di dipendenti, indipendentemente dalle mansioni svolte, poteva venire a conoscenza di dati personali, anche relativi all'esecuzione della prestazione lavorativa da parte dei colleghi (quali permessi accordati in base alla l. n. 104/1992, permessi studio, documentazione riguardante sussidi per l'accesso a mense scolastiche o borse di studio ovvero contestazioni disciplinari).

L'Autorità ha accertato la violazione delle disposizioni relative alle misure minime di sicurezza del sistema di protocollazione e gestione documentale, poiché non erano stati individuati e configurati i profili di autorizzazione dei diversi incaricati, così da limitare l'accesso ai dati relativi ai dipendenti al solo personale assegnato a questo compito. Di qui le prescrizioni impartite, per segmentare la visibilità dei documenti e dei fascicoli relativi al personale ai soli dipendenti incaricati del trattamento dei dati; è stato altresì prescritto lo

svolgimento di un'attività formativa indirizzata al personale della sede che ha fatto uso del sistema di gestione documentale, illustrandone compiutamente le funzionalità e le implicazioni in materia di protezione dei dati.

13.2. DATI BIOMETRICI E RAPPORTO DI LAVORO

Con riferimento al trattamento di dati biometrici per la rilevazione delle presenze dei lavoratori il Garante ha ribadito il proprio consolidato orientamento che reputa, di regola, eccedente l'utilizzo di informazioni biometriche per finalità di ordinaria gestione del rapporto di lavoro e, segnatamente, per la commisurazione dell'orario di servizio prestato (cfr. punto 4. provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. web n. 1364099] e punto 7. provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. web n. 1417809]).

Tale orientamento -condiviso da una recente giurisprudenza di merito (Trib. Prato, 19 settembre 2011) e coerente con quanto affermato nel Parere n. 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato in data 27 aprile 2012, dal Gruppo Art. 29 secondo cui "*il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico*"- si affianca a quello, esso pure consolidato, secondo cui è invece di regola lecito l'utilizzo di tali dati per presidiare l'accesso ad "aree sensibili", anche in considerazione della natura delle attività ivi svolte.

In termini generali, si segnala, altresì, che è risultato frequente l'inadempimento dell'obbligo di notificazione al Garante dei trattamenti effettuati con l'impiego di dispositivi biometrici (cfr. artt. 37 e 163 del Codice).

Venendo alla casistica, in sede di verifica preliminare (*ex* art. 17 del Codice), un comune ha sottoposto al Garante l'installazione di un sistema di rilevazione biometrica basato sulla lettura delle impronte digitali per finalità di rilevazione delle presenze dei dipendenti, volto ad impedire il reiterarsi di fenomeni di uso improprio del *badge* individuale, oggetto di un'indagine dell'autorità giudiziaria. Il Garante ha ritenuto il trattamento non conforme ai princìpi di necessità, pertinenza e non eccedenza (in relazione

agli artt. 3, 11, comma 1, lett. *d*), del Codice), posto che l'ente locale non aveva dato prova dell'insufficienza delle ordinarie modalità di controllo della presenza dei lavoratori -con riferimento sia a sistemi fisici sia a misure tecnico-organizzative di agevole implementazione- in alternativa ai più invasivi sistemi biometrici, l'utilizzo dei quali potrebbe peraltro rivelarsi, in sé, di scarsa utilità nel contrasto dell'assenteismo ove non accompagnata da un'efficace opera di controllo e verifica da parte del datore di lavoro (provv. 31 gennaio 2013 [doc. web n. 2304669]).

In un altro caso il Garante ha accertato che presso un cantiere edile per la ristrutturazione di un immobile, l'accesso delle maestranze ivi impiegate era consentito -unitamente ad altre modalità di accertamento dell'identità dei lavoratori- previa identificazione biometrica effettuata da apposito sistema basato sulla rilevazione della geometria della mano e successiva estrazione del relativo *template*, poi conservato in un unico *database*. Considerata la mancanza di specifici elementi in relazione alla concreta attività svolta dai titolari del trattamento ed alla luce dell'esistenza di concorrenti procedure di identificazione delle maestranze, il Garante non ha ritenuto lecito il sistema biometrico utilizzato (provv. 13 settembre 2012 [doc. web n. 1927456]).

13.3. TRATTAMENTO DI DATI IDONEI A RIVELARE LE OPINIONI SINDACALI

Tra le decisioni relative all'utilizzo di dati personali nell'ambito della gestione del rapporto di lavoro, merita di essere menzionato il provvedimento che ha ritenuto illecito il trattamento effettuato dalla direzione di una casa circondariale di dati sensibili ai sensi dell'art. 4, comma 1, lett. *d*), del Codice, segnatamente dei nominativi del personale di polizia penitenziaria che aveva preso parte ad una manifestazione sindacale (provv. 29 novembre 2012 [doc. web n. 2192643]).

Nella vicenda in esame, il trattamento dei dati sensibili nell'ambito della gestione del rapporto di lavoro, pur se (in astratto) consentito ai fini dell'instaurazione di un eventuale procedimento disciplinare a carico di alcuno dei partecipanti (artt. 20, comma 1, 112, comma 2, lett. *g)*, del Codice nonché decreto del Ministro della giustizia 12 dicembre 2006 n. 306, "Regolamento sulla disciplina del trattamento dei dati sensibili e giudiziari da parte del

Ministero della giustizia"), non è risultato lecito (ai sensi degli artt. 11, comma 1, lett. *a)* e 20, comma 1, del Codice) non essendosi rinvenuti i presupposti per disporre alcun procedimento disciplinare a carico dei partecipanti alla manifestazione, né potendo la mera indizione e partecipazione ad una manifestazione sindacale configurare di per sé alcun illecito per l'ordinamento, alla luce della fondamentale libertà di riunione riconosciuta dall'art. 17 della Costituzione nonché dall'art. 19, l. n. 395/1990 che, nell'ambito dell'ordinamento del Corpo di polizia penitenziaria, stabilisce le norme di comportamento nel godimento dei diritti politici, civili e sindacali.

Con il medesimo provvedimento è stato vietato alla direzione della casa circondariale di trattare ulteriormente i dati relativi ai nominativi dei partecipanti alla manifestazione, con loro conservazione per esigenze di tutela dei diritti in sede giudiziaria, ed è altresì stato prescritto di portare a conoscenza dei soggetti cui eventualmente i dati riferiti agli interessati fossero stati comunicati il contenuto del provvedimento, con particolare riguardo al profilo dell'inutilizzabilità dei dati sensibili dei lavoratori.

13.4. INPS

Nel settore oggetto di competenza dell'Istituto si evidenziano essenzialmente casi riguardanti singoli trattamenti.

In dettaglio, il Garante è intervenuto in un caso in cui un cittadino si era visto recapitare, da una filiale dell'Inps, il verbale di accertamento dell'invalidità civile, contenuto in una busta al cui esterno una timbratura rendeva esplicita la sua condizione di disabile.

Al riguardo, l'Autorità ha ribadito che la normativa in materia di protezione dati prevede che i plichi postali non devono recare, sulla parte esterna, segni o indicazioni tali da consentire a soggetti estranei di desumere il contenuto delle comunicazioni ovvero, anche indirettamente, informazioni idonee a rivelare lo stato di salute del destinatario. L'ente previdenziale ha pertanto disposto che le buste utilizzate per l'invio di documentazione sanitaria non rechino indicazioni del genere (nota 18 giugno 2012).

In un'altra occasione, una segnalazione lamentava che una sede dell'Inps aveva inviato una comunicazione circa l'esito della visita per il riconoscimento dell'invalidità civile ad un

soggetto diverso dall'interessato. Il Garante ha invitato l'Istituto ad adottare misure idonee ad evitare il ripetersi della vicenda. Peraltro, in relazione alla comunicazione di dati idonei a rivelare lo stato di salute a persona diversa dell'interessato, l'Ufficio si è riservato, con autonomo procedimento, di verificare i presupposti per contestare la violazione amministrativa (nota 3 settembre 2012).

A seguito di autonomi accertamenti effettuati dall'Ufficio, è stato riscontrato che sul sito istituzionale di una provincia erano consultabili e accessibili a chiunque le graduatorie di disabili, ai fini del collocamento obbligatorio. Il Garante, nel richiamare le indicazioni fornite nelle linee-guida del 2 marzo 2011 [doc. web n. 1793203], ha evidenziato il divieto di diffondere informazioni idonee a rivelare lo stato di salute, che possono essere messe a disposizione *online* solo con modalità che ne impediscano la libera consultabilità in internet. Le amministrazioni possono, pertanto, pubblicare *online* elenchi o documentazione purché accessibili ai soli soggetti richiedenti (e per le sole finalità previste dalla normativa di riferimento) ovvero a coloro che vi abbiano interesse per la tutela di situazioni giuridicamente rilevanti (a tali fini attribuendo per es. idonee credenziali di accesso, quali *username* o *password*, n. di protocollo, ovvero ancora predisponendo, nei siti istituzionali, aree ad accesso selezionato).

A seguito dell'intervento del Garante, la provincia ha rimosso dal sito gli elenchi oggetto di segnalazione, ma l'Ufficio si è riservato di accertare con autonomo procedimento la violazione del divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (nota 1° ottobre 2012).

Un ufficio periferico dell'Istituto nazionale previdenza sociale ha investito l'Autorità, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, di una richiesta volta a consentire la comunicazione ad un ufficio provinciale del Ministero del lavoro e delle politiche sociali delle informazioni personali contenute nell'estratto contributivo relativo ad alcuni lavoratori (individuati nominativamente) ai sensi dell'art. 3, comma 5, del d.m. 27 ottobre 2004 (disciplina attuativa dell'art. 47, d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, nella l. 24 novembre 2003, n. 326, "Benefici previdenziali per i lavoratori esposti all'amianto"). La comunicazione sarebbe stata effettuata nell'ambito delle finalità istituzionali delle direzioni

provinciali del lavoro, cui il menzionato art. 3 attribuisce un'attività di indagine volta sia a consentire la ricostruzione del *curriculum* professionale dei lavoratori esposti all'amianto in vista del conseguimento dei benefici di legge, sia alla individuazione dell'effettivo datore di lavoro che nel tempo ha provveduto ai versamenti contributivi, nei casi in cui il datore di lavoro, cessato o fallito, sia divenuto irreperibile. Il Garante, riconosciute le finalità istituzionali della comunicazione ha accolto l'istanza, consentendo la comunicazione dei soli dati pertinenti e non eccedenti, funzionali alla redazione del *curriculum* professionale da trasmettere poi successivamente all'Inail, ossia la denominazione del datore di lavoro, il periodo lavorativo e le mansioni, con eventuale indicazione del reparto del lavoratore (provv. 21 marzo 2012 [doc. web n. 1885290]).

13.5. TRATTAMENTO DI DATI PERSONALI E VALUTAZIONI DELLA RICERCA UNIVERSITARIA

Il Presidente dell'Autorità è intervenuto nel dibattito pubblico circa la possibilità di diffondere -con la particolare modalità della pubblicazione *online*- le valutazioni effettuate dall'Anvur (Agenzia nazionale per la valutazione del sistema universitario e della ricerca) sulle attività svolte dalle strutture di ricerca (intervento 3 novembre 2012 [doc. web n. 2086888]). La legittimità del regime di pubblicità dei "prodotti della ricerca" non può che essere valutata alla luce del principio di trasparenza dell'attività amministrativa, preordinato alla realizzazione del buon andamento e dell'imparzialità dell'amministrazione e attuato nei limiti previsti dalla normativa vigente (anche di origine comunitaria) che ne disciplina oggetto, scopi e modalità, in vista del necessario bilanciamento con le esigenze di tutela della riservatezza delle persone. Posto che, in particolare, il Codice consente ai soggetti pubblici di diffondere *online* dati personali solo qualora una norma di legge o di regolamento lo preveda espressamente (art. 19, comma 3) e che l'oggetto della attività valutativa dell'Anvur è, in base alle norme istitutive, la qualità delle strutture universitarie e degli enti di ricerca (non invece dei singoli ricercatori) al fine di predisporre l'allocazione delle risorse finanziarie disponibili, non risulta ancorata ad una idonea base giuridica la pubblicazione in rete dei dati relativi alle valutazioni dei singoli ricercatori. Peraltro, considerato anche che oggetto di valutazione è un numero limitato di pubblicazioni (tre), il giudizio così espresso e reso pubblico potrebbe non

costituire lo strumento più appropriato per rappresentare con modalità trasparenti il merito (o demerito) della produzione scientifica di ciascuno (note 19 settembre 2012).

13.6. PUBBLICAZIONE IN INTERNET DI DATI PERSONALI RELATIVI A LAVORATORI

Numerose sono le segnalazioni ad opera di pubblici dipendenti (o candidati nel settore del pubblico impiego) che lamentano la pubblicazione di dati eccedenti o la persistente pubblicazione in internet, tramite i siti web istituzionali ovvero mediante l'albo pretorio *online*, di vicende personali in difformità dalle previsioni normative.

Esiti di prove di concorso

A tal proposito, può segnalarsi la vicenda di un candidato non ammesso (unitamente ad altri) a sostenere la prova orale di un concorso bandito da un comune nel 2008 e rispetto al quale, a distanza di anni, persistevano sul sito web istituzionale dell'ente reperibili tramite i comuni motori di ricerca, i dati nominativi dei candidati e gli esiti delle prove intermedie sostenute dai partecipanti, compreso il segnalante. Nel premettere che la disciplina di settore dispone che siano pubblicate nell'albo pretorio dell'ente le sole graduatorie definitive dei vincitori di concorso presso gli enti locali territoriali (art. 15, comma 6-*bis*, d.P.R. 9 maggio 1994, n. 487, regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi), il Garante ha ritenuto illecita la persistente pubblicazione in internet dei dati in parola (artt. 11, comma 1, lett. *a)* e *d)* e 19, comma 3, del Codice; a conferma di altra decisione del Garante cfr., nello stesso senso, Cass. civ., sez. I, 20 luglio 2012, n. 12726). È stato pertanto vietato al comune di diffondere ulteriormente - sia attraverso la pubblicazione nell'albo pretorio *online* che in qualsiasi altra area del sito web istituzionale- i dati personali contenuti nella graduatoria provvisoria del concorso (provv. 6 dicembre 2012 [doc. web n. 2223278]).

In presenza di segnalazioni concernenti l'avvenuta pubblicazione sul sito web del Ministero della giustizia di alcuni dati personali -segnatamente, nomi, cognomi, data di nascita ed esito delle prove scritte riferiti ai candidati del concorso da uditore giudiziario (con la precisazione, per i non ammessi alle prove orali, del giudizio di inidoneità)-, l'Ufficio ha formulato richiesta di informazioni al Ministero evidenziando, tra l'altro, che la disciplina di settore, pur risalente,

si limita a prevedere che "*il risultato completo delle prove scritte sarà reso di pubblica ragione mediante foglio da affiggersi nei locali del Ministero*" (art. 13, ult. comma del r.d. 15 ottobre 1925, n. 1860 - "Modificazioni al regolamento per il concorso di ammissione in magistratura contenuto nel r.d. 19 luglio 1924, n. 1218"). Il Ministero, che aveva prontamente rimosso i dati oggetto di segnalazione dal sito, sulla scorta delle osservazioni del Garante (cfr. linee-guida 2 marzo 2011, cit. punto B.1., nonché provv. 19 aprile 2007 [doc. web n. 1407101], punto 5.), ha quindi provveduto ad introdurre gli accorgimenti tecnici -quali la consultabilità in una sezione del sito web istituzionale degli esiti concorsuali previo inserimento di credenziali individuali, individuate nel codice fiscale e del numero tessera fornita a ciascun candidato in occasione dell'espletamento delle prove- volti ad impedire l'indiscriminata visibilità degli esiti delle prove in internet (nota 23 marzo 2012).

Albo pretorio *online*

Con riferimento alla pubblicazione di atti e documenti nell'albo pretorio *online*, l'Autorità ha definito alcuni procedimenti relativi alla pubblicazione da parte di soggetti pubblici (solitamente enti locali) di atti e documenti riguardanti dipendenti. In alcuni casi la pubblicazione concerneva riferimenti allo stato di salute del lavoratore, dando luogo ad una diffusione di dati vietata ai sensi dell'art. 22, comma 8, del Codice (nonché sanzionata dall'art. 162, comma 2-*bis*, del Codice). Al riguardo, pur potendo le deliberazioni degli organi comunali, consiliari o giuntali, formare oggetto di pubblicazione, l'ente locale titolare aveva l'obbligo di oscurare i riferimenti allo stato di salute dell'interessato (in un caso, peraltro, contenuti in un verbale allegato al provvedimento).

In tali fattispecie è stato ribadito che, alla luce della disciplina in materia di protezione dei dati personali -e conformemente a quanto stabilito nelle linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011 [doc. web n. 1793203]- nell'adempimento degli obblighi di pubblicazione *online* di atti e provvedimenti amministrativi aventi effetto di pubblicità legale, le amministrazioni possono pubblicare dati personali, anche tratti da atti e documenti amministrativi, qualora "*tale divulgazione, che deve essere sempre sorretta da un'adeguata motivazione, costituisca un'operazione strettamente necessaria al perseguimento delle finalità assegnate all'amministrazione da specifiche leggi o regolamenti*",

salvo in ogni caso il generale e già menzionato divieto di diffusione dei dati relativi allo stato di salute degli interessati (cfr. punto 2.2. linee- guida cit.) (note 12 aprile e 4 luglio 2012).

In altri casi, invece, quando gli atti pubblicati dagli enti locali sono rimasti disponibili sui siti istituzionali oltre il tempo consentito dalla disciplina di settore, con specifico riferimento all'intervallo temporale di diffusione, è stata rilevata l'illiceità del trattamento (artt. 11, comma 1, lett. *a)* e 19, comma 3, del Codice). Infatti, la persistenza delle informazioni personali nell'albo pretorio *online* oltre il termine consentito dalla legge -senza che gli atti o le delibere fossero privati degli elementi identificativi degli interessati- ha reso illecita la diffusione dei dati personali in quanto priva (per il periodo successivo ai quindici giorni previsti dall'art. 124, d.lgs. n. 267/2000 per la pubblicazione nell'albo pretorio) di idonei presupposti normativi (nota 4 luglio 2012).

Come peraltro già chiarito al punto 5.2. delle menzionate linee-guida, trascorsi i periodi di tempo individuati dalla legge per la pubblicazione di atti e provvedimenti amministrativi, i medesimi "*devono essere rimossi dal web o privati degli elementi identificativi degli interessati ovvero, in alternativa, laddove l'ulteriore diffusione dei dati sia volta a soddisfare esigenze di carattere storico-cronologico, gli stessi vanno sottratti all'azione dei comuni motori di ricerca, ad esempio, inserendoli in un'area di archivio consultabile solo a partire dal sito stesso o in un'area ad accesso riservato*" (provv. 23 febbraio 2012 [doc. web n. 1876679]).

Numerose sono state le segnalazioni aventi ad oggetto la pubblicazione sui siti web istituzionali di istituti scolastici, nonché di altri uffici periferici del Ministero dell'istruzione dell'università e della ricerca, di graduatorie di dati personali concernenti il personale docente ovvero il personale amministrativo tecnico ed ausiliario (cd. "ATA") recanti, oltre ai punteggi maturati ed alle generalità degli interessati, anche dati ulteriori quali il numero di codice fiscale, il numero di figli a carico ed i recapiti degli interessati (in particolare nota 8 agosto 2012).

Al riguardo, nelle menzionate linee-guida del 2 marzo 2011 [doc. web n. 1793203] è stato precisato che, in applicazione dei princìpi di liceità, correttezza nonché di pertinenza e non eccedenza (art. 11, comma 1, lett. *a)* e *d)*, del Codice), deve ritenersi eccedente la pubblicazione di dati quali, il recapito di telefonia fissa o mobile, l'indirizzo dell'abitazione o dell'e-mail, i titoli di studio, il codice fiscale.

Nel ribadire che, nello svolgimento di attività istituzionali, la pubblicazione *online* di dati personali deve avvenire, oltre che nel rispetto del Codice, anche osservando la legge e i regolamenti che tale pubblicazione eventualmente prevedono (*ex* artt. 18, 19, comma 3 e 25, del Codice), l'Ufficio ha formulato una richiesta di informazioni al ministero, anche al fine di chiarire il ruolo svolto dagli enti periferici o istituti scolastici nella pubblicazione degli elenchi in esame, i presupposti di legittimità relativi alla diffusione e all'osservanza dei princìpi di necessità (art. 3, del Codice) nonché di pertinenza e non eccedenza della tipologia delle informazioni oggetto di diffusione rispetto alla legittima finalità perseguita (art. 11, comma 1, lett. *d)*, del Codice), oltre che per individuare l'arco temporale durante il quale i menzionati dati personali possono restare visibili in internet.

Merita infine di essere segnalato il provvedimento con il quale il Garante ha vietato la pubblicazione, sul sito di un ateneo, del decreto di annullamento e revoca dell'affidamento di un insegnamento a contratto, risultata non conforme alla disciplina di settore e quindi in violazione del principio di liceità del trattamento di cui all'art. 11, comma 1, lett. *a*) del Codice. Ciò anche in ragione della considerazione che la pubblicazione del provvedimento in parola, contenente le ragioni dell'annullamento del contratto, fosse comunque eccedente rispetto alle finalità perseguite dall'università, in quanto visibile ad una cerchia di soggetti assai più ampia rispetto agli interessati (provv. 12 aprile 2012 [doc. web. 1896533]).

13.7. CONTROLLO A DISTANZA DEI LAVORATORI

La materia del controllo a distanza dei lavoratori (in particolare per il tramite di sistemi di videosorveglianza) e del connesso trattamento di dati personali continua a formare oggetto di numerose segnalazioni indirizzate all'Autorità e di verifiche effettuate *in loco* anche attraverso la Guardia di finanza nonché, nei casi di inosservanza dell'art. 4, l. n. 300/1970, di trasmissione all'Autorità giudiziaria per l'accertamento di violazioni penalmente rilevanti.

In argomento, con riferimento a quanto esposto nella Relazione 2011 (p. 121), è stata respinta dal Tribunale di Roma il 21 gennaio 2013 l'impugnazione avverso il provvedimento del Garante 21 luglio 2011 [doc. web n. 1829641], con il quale sono state ritenute illegittime la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione in internet dei dipendenti di una società di primaria rilevanza.

Videosorveglianza

A seguito degli accertamenti effettuati presso un *call center*, il Garante ha vietato il trattamento dei dati rilevati mediante un sistema di videosorveglianza ivi installato in grado di captare anche le conversazioni dei dipendenti, in violazione dell'art. 4, l. n. 300/1970 (provv. 4 ottobre 2012 [doc. web n. 2066968]). Provvedimenti di analogo contenuto sono stati adottati, in relazione a trattamenti effettuati, in assenza delle garanzie dettate dall'art. 4, l. n. 300/1970, mediante sistemi di videosorveglianza da parte di un hotel (provv. 25 ottobre 2012 [doc. web n. 2212826]) e di un esercizio commerciale (provv. 25 ottobre 2012 [doc. web n. 2212623]).

Il Garante ha dichiarato illecito anche un trattamento effettuato tramite un sistema di videosorveglianza, installato per finalità antitaccheggio presso un negozio, disponendo il blocco del trattamento dei dati. La telecamera riprendeva anche l'area nella quale è posto l'apparecchio per la rilevazione delle presenze dei lavoratori.

In questo caso, è stata ritenuta inidonea l'informativa fornita agli interessati (pur nelle forme semplificate indicate dall'Autorità nel provvedimento generale dell'8 aprile 2010 [doc. web n. 1712680]) ed è stata altresì riscontrata la possibilità (dal punto di vista tecnico) di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali (in violazione dei princìpi di liceità e correttezza nel trattamento). Un ulteriore profilo di illiceità del trattamento è stato ravvisato nella circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa dal titolare del trattamento, è risultato privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773 (tulps)), con esigenza ribadita sia in relazione al servizio antitaccheggio sia in relazione al servizio di televigilanza (cfr. art. 3, comma 2, lett. *d)*, e lett *f)* d.m. 1° dicembre 2010, n. 269), come peraltro stabilito dal consolidato indirizzo interpretativo della giurisprudenza di legittimità secondo cui "*ogni forma di attività imprenditoriale di vigilanza e custodia di beni per conto terzi esige la licenza del prefetto, indipendentemente dalle modalità operative con le quali viene espletata*" (cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821 e ivi ulteriori richiami) (provv. 17 gennaio 2013 [doc. web n. 2291893]).

Ascolto e montaggio delle telefonate dei lavoratori

L'Autorità ha effettuato accertamenti anche in relazione alla registrazione e riascolto delle telefonate effettuate dai lavoratori del *call center* gestito da una cooperativa -la quale eroga

anche il servizio di prenotazione telefonica di prestazioni sanitarie in una regione- nonché al monitoraggio della loro condotta mediante l'analisi del numero e della durata delle conversazioni.

Al riguardo, poiché la registrazione e il riascolto del contenuto delle comunicazioni precedentemente registrate, pur per soddisfare esigenze organizzative o produttive, consentono il controllo a distanza dell'attività dei lavoratori, il Garante ha rilevato che il mancato assolvimento degli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 (fatto salvo dall'art. 114 del Codice) riverbera i propri effetti anche sulle operazioni di trattamento dei dati, risultate perciò in violazione dell'art. 11, comma 1, lett. *a)*, del Codice (provv. 1° agosto 2012 [doc. web n. 1923325]; in merito v. provv. 9 febbraio 2011 [doc. web n. 1797032]). Analoga la valutazione sul monitoraggio, in base al loro numero o durata, delle conversazioni di ciascun operatore telefonico -che ha talvolta determinato l'adozione di provvedimenti disciplinari nei confronti dei soci lavoratori- non essendo stati posti in essere dalla società gli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970.

Geolocalizzazione

Nonostante le prescrizioni impartite in via generale dal Garante con il provvedimento 4 ottobre 2011, n. 370 [doc. web n. 1850581], continuano a formare oggetto di segnalazione trattamenti di dati personali riferiti ai lavoratori effettuati mediante sistemi di geolocalizzazione installati su veicoli aziendali.

In un caso, con riguardo all'impiego di tali sistemi su veicoli assegnati a guardie giurate, il Garante ha ritenuto che il sistema di localizzazione in uso poteva contribuire al conseguimento delle legittime finalità dichiarate dal datore di lavoro, incrementando nel caso di specie anche la sicurezza dei dipendenti; nondimeno, l'impiego di tali strumenti deve avvenire nel rispetto della normativa in materia di protezione dei dati personali. Considerato che il sistema installato consentiva di monitorare a distanza -ancorché non in modo continuo- la posizione del veicolo e, quindi, indirettamente, del lavoratore cui lo stesso era assegnato, il Garante ha rilevato che la società titolare del trattamento non aveva dato attuazione agli adempimenti necessari ai sensi dell'art. 4, comma 2, della l. n. 300/1970, così come richiamato dall'art. 114 del Codice, né reso l'informativa ai dipendenti ai sensi dell'art. 13 del Codice (provv. 1° agosto 2012 [doc. web n. 1923293]).

Nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha invece ritenuto lecito il trattamento di dati personali da parte di una società concessionaria del servizio di trasporto pubblico locale tramite l'installazione di un dispositivo -da apporre sul parabrezza delle vetture e annoverabile tra i cd. "*video event data recorder*" che consente di registrare e -al verificarsi di predeterminate "anomalie"- conservare, immagini relative sia all'interno che all'esterno del veicolo. Le finalità perseguite dalla società (salvaguardia del patrimonio aziendale nonché ricostruzione della dinamica di eventuali sinistri in vista della tutela dei diritti in giudizio) e le concrete modalità di trattamento dei dati (esclusione dell'immagine del conducente dall'angolo di ripresa, offuscamento dei volti di soggetti terzi non coinvolti negli eventi) sono state infatti ritenute conformi ai princìpi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *d)*, del Codice). L'Autorità ha ritenuto giustificata la conservazione dei dati registrati per ventiquattro mesi, reputando però eccedente, anche alla luce della sua possibile rilevanza penale (cfr. artt. 617, 617-*bis* e 623-*bis* c.p.) rispetto alle finalità rappresentate, la raccolta e conservazione -prospettata dalla società- di registrazioni della voce delle persone a bordo del veicolo.

I trattamenti effettuati nonché la presenza del dispositivo dovranno comunque essere adeguatamente resi noti, anche attraverso apposita rappresentazione grafica, a tutte le categorie di persone (dipendenti, utenti del servizio ed eventuali terzi) che potrebbero essere interessate dal trattamento (provv. 29 novembre 2012 [doc. web n. 2257616]).

14. Le attività economiche

14.1. Settore bancario

A seguito del provvedimento, adottato il 12 maggio 2011 in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (in G.U. 3 giugno 2011, n. 127 [doc. web n. 1813953]), il Garante ha proseguito nell'attività di collaborazione già avviata con gli operatori del settore.

Con il citato provvedimento -adottato a seguito di segnalazioni e reclami con cui i clienti di alcuni istituti bancari avevano lamentato l'avvenuta effettuazione, presumibilmente da parte di alcuni dipendenti, di accessi indebiti ai loro dati personali (in particolare, informazioni bancarie), poi comunicati a loro insaputa a terzi che li avevano utilizzati per scopi personali (soprattutto nell'ambito di procedimenti di separazione personale e in procedure esecutive)- l'Autorità ha prescritto l'adozione di misure rigorose volte ad impedire illecite operazioni di trattamento ai danni degli interessati. In particolare, è stato stabilito che ogni operazione di accesso ai dati dei clienti, effettuata dagli incaricati del trattamento (sia che comporti movimentazione di denaro, sia di semplice consultazione), dovrà essere tracciata attraverso una serie di elementi, così da consentire alla stessa banca di conoscere chi abbia effettuato il trattamento dei dati e il momento in cui ciò è avvenuto.

A seguito di richieste pervenute da Associazione bancaria italiana (Abi) e Poste Italiane S.p.A., l'Autorità nel 2012 ha intrapreso con tali soggetti un'attività di collaborazione, ancora in corso, volta a fornire chiarimenti in ordine alla corretta applicazione del provvedimento stesso.

Nel corso del 2011 le banche, al fine di contrastare sempre più diffusi fenomeni criminali, hanno rappresentato la necessità di avvalersi di sistemi di videosorveglianza dotati di un *software* "anticamuffamento", in grado di permettere l'individuazione di eventuali rapinatori senza dover ricorrere a strumenti comportanti la rilevazione di impronte digitali. In tale occasione l'Abi, in qualità di rappresentante delle banche, ha chiesto all'Autorità di valutare se le proprie associate fossero effettivamente tenute a presentare una richiesta di verifica preliminare per procedere all'attivazione di tali sistemi.

All'esito dell'attività istruttoria, l'Ufficio ha rappresentato all'Abi (nota 19 dicembre 2011) che il sistema, così come descritto dai titolari del trattamento, sembrerebbe rilevare solo eventuali situazioni di camuffamento, senza procedere ad operazioni di riconoscimento del volto basate sul confronto con immagini contenute in banche dati fotografiche. Il trattamento, pertanto, non è stato ritenuto soggetto a verifica preliminare, sia perché la raccolta dell'immagine dell'interessato non aggiunge nulla di ulteriore rispetto a quanto avviene con l'impiego di un normale sistema di videosorveglianza, sia perché l'elaborazione delle immagini per la verifica di eventuali camuffamenti non prevede la loro associazione ad altre immagini contenute in banche dati fotografiche.

Inoltre, da alcune banche sono pervenute anche richieste di verifica preliminare volte all'attivazione di un sistema comportante la rilevazione dei dati biometrici degli interessati per consentire alla clientela di accedere alle cassette di sicurezza -in modalità *self service*- 24 ore su 24 tutti i giorni della settimana. Il sistema sarebbe stato attivato, previo rilascio di apposito consenso informato, solo su specifica richiesta del cliente, con acquisizione di una sua impronta digitale attraverso un apposito lettore in grado di generare un algoritmo matematico univoco ed irripetibile, a sua volta memorizzato solo su una *smartcard* consegnata all'interessato unitamente ad un *pin*. Per i clienti che non avessero inteso avvalersi del sistema, sarebbero state previste modalità alternative di registrazione e di accesso al servizio di cassette di sicurezza, tramite l'inserimento di una carta magnetica e la digitazione del codice personale. All'esito dell'attività istruttoria, il Garante ha adottato singoli provvedimenti (provv. 13 settembre 2012 [doc. web n. 1927441] e provv. 18 ottobre 2012 [doc. web n. 2212554]) con i quali, nel ritenere lecita la finalità perseguita dalle banche e proporzionato il trattamento dei dati personali, ha prescritto agli istituti di credito l'adozione di specifici accorgimenti e, in particolare, di conservare una descrizione scritta dell'intervento effettuato dall'installatore, che attesti anche la conformità del sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'Allegato B. al Codice), nonché di notificare al Garante il trattamento dei dati biometrici prima dell'inizio delle operazioni di trattamento (art. 37, comma 1, lett. *a*), del Codice).

Con riferimento ad una ipotesi di cessione di ramo di azienda, l'Autorità si è espressa sull'istanza di una società operante nel settore del credito al consumo con la quale veniva

chiesto, in via principale, l'esonero dall'obbligo di rendere l'informativa agli interessati (tra cui, in particolare, i dipendenti e i clienti della società cedente) ed in via subordinata - considerata la particolare fattispecie della cessione del ramo di azienda- di poter rendere l'informativa con modalità semplificate, in particolare con quella prevista "*per la notizia della cessione dei rapporti giuridici in blocco, dall'art. 58 del testo unico delle leggi in materia bancaria e creditizia*". L'istanza rappresentava che le modalità ordinarie di informativa, per il numero elevatissimo di interessati (oltre 215.000 clienti), avrebbe comportato l'impiego di mezzi manifestamente sproporzionati.

L'Autorità, nel caso di specie, ha considerato che l'operazione negoziale intercorsa tra le due società (la suddetta cessione di ramo d'azienda) fosse regolata dall'art. 58, comma 7, del d.lgs. 1° settembre 1993, n. 385 (testo unico delle leggi in materia bancaria e creditizia T.u.b.) e -anche alla luce di un precedente provvedimento, in ragione della peculiarità della disciplina, della tipologia dei dati ceduti e dell'immutata finalità del trattamento- ha valutato come prevalente, rispetto alla riservatezza dei soggetti medesimi, l'interesse della società cedente alla comunicazione dei dati personali alla società cessionaria (v. art. 24, comma 1, lett. *g*), del Codice). Pertanto ha ritenuto che la comunicazione dei dati personali tra le due società potesse considerarsi lecita, anche in assenza del consenso degli interessati.

Di conseguenza, l'Autorità ha consentito alla società richiedente di rendere l'informativa agli interessati, contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice, mediante la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, contestualmente alla pubblicazione dell'avviso di cessione "*in blocco*" dei rapporti giuridici previsto dall'art. 58 del T.u.b, prescrivendo altresì ad entrambe le società coinvolte, quali ulteriori "*misure appropriate*" (art. 13, comma 5, lett. *c*), del Codice), di pubblicare sui propri siti web un annuncio recante i contenuti dell'informativa (provv. 5 luglio 2012 [doc. web n. 1913790]).

14.2. SETTORE ASSICURATIVO

L'Autorità è stata chiamata a pronunciarsi su un'istanza di bilanciamento di interessi (art. 24, comma 1, lett. *g)*, del Codice), presentata da alcune società appartenenti al medesimo

gruppo assicurativo e operanti nel ramo danni, in relazione al trattamento dei dati non sensibili dei molteplici soggetti (quali contraenti, danneggiati, periti, medici, legali, testimoni, carrozzieri) coinvolti, a vario titolo, nelle procedure di liquidazione dei sinistri. L'istanza -formulata nell'ambito di un progetto in fase di implementazione presso gran parte delle consociate europee finalizzato, tra l'altro, all'individuazione attraverso l'utilizzo di specifici modelli previsionali di possibili richieste di risarcimento danni fraudolente- avrebbe trovato fondamento, a detta delle società, nel loro legittimo interesse a tutelarsi contro fenomeni fraudolenti (oltre che nell'oggettiva impossibilità di acquisire un preventivo consenso da parte di tutti gli interessati), suffragata anche dalla normativa di settore. L'Autorità, nel riconoscere l'indubbia meritevolezza delle finalità perseguite, ha tuttavia accolto solo parzialmente l'istanza, ravvisando idonei presupposti per il richiesto bilanciamento esclusivamente in relazione ai soggetti coinvolti, a vario titolo, nelle procedure di risarcimento danni da responsabilità civile connessa alla circolazione di veicoli a motore; è stato precisato, tuttavia, che nulla osta, in linea di principio, a che le società trattino i dati personali degli interessati, per le finalità indicate e in relazione all'intero ramo danni, in presenza di altro presupposto di liceità di cui all'art. 24 del Codice (provv. 24 gennaio 2013 [doc. web n. 2352902]).

14.3. ALTRE ATTIVITÀ IMPRENDITORIALI

Nel 2012 il Garante ha intrapreso una importante attività di collaborazione con l'Autorità per l'energia elettrica e il gas in vista della realizzazione di una banca dati contenente i dati identificativi dei clienti delle imprese del settore, cd. "sistema informativo integrato", previsto da specifica normativa (art. 1-*bis*, l. 13 agosto 2010, n. 129, di conversione in legge, con modificazioni, del d.l. 8 luglio 2010, n. 105 recante "Misure urgenti in materia di energia"). Tale sistema è stato previsto a seguito della liberalizzazione del mercato dell'energia elettrica e del gas, che consente a tutti i clienti di scegliere liberamente il proprio fornitore. La banca dati, istituita presso Acquirente Unico S.p.A., ha soltanto lo scopo di risolvere il problema creato dal passaggio dei clienti da un fornitore all'altro in presenza di morosità pregresse (cd. "turisti energetici").

Nel corso dell'attività di collaborazione sono stati esaminati i princìpi e le regole da applicare affinché il trattamento posto in essere risulti conforme al Codice: l'informativa ai sensi dell'art. 13 del Codice; l'acquisizione del consenso, rispetto al quale è applicabile la fattispecie di esonero previsto dall'art. 24, comma 1, lett. *a*), del Codice, considerato che il trattamento posto in essere è espressamente previsto da una specifica norma di legge; i tempi di conservazione non superiori a quelli necessari agli scopi per i quali sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. *c*), del Codice). Tuttavia sono risultati ancora in fase di definizione specifici aspetti, tra cui l'individuazione dei dati personali oggetto di trattamento all'interno del sistema e delle informazioni concernenti eventuali inadempimenti contrattuali dei clienti. La definizione di tali contenuti avverrà con delibera del Collegio dell'Autorità per l'energia elettrica e il gas, a seguito di una consultazione pubblica avviata dalla stessa Autorità di settore, sicché il Garante, pur individuando misure ed accorgimenti affinché il trattamento sia effettuato in conformità al Codice, si è riservato di formulare un formale parere all'esito dell'elaborazione del documento finale (nota 2 maggio 2012).

14.4. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Nel corso dell'anno, il Garante si è pronunciato in relazione ad una serie di istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società del settore privato per l'allungamento dei tempi di conservazione delle immagini registrate e con riferimento a sistemi cd. "intelligenti".

Con provvedimento del 12 gennaio 2012 [doc. web n. 1875004], l'Autorità si è pronunciata sulla richiesta (art. 17 del Codice) di attivazione di un impianto di videosorveglianza cd. "intelligente", provvisto anche di un sistema di captazione audio, presso una centrale termoelettrica di interesse nazionale -stante la sua considerevole capacità produttiva- che era stata bersaglio, nel corso del tempo, di vari atti illeciti. La società stessa ha quindi scelto di dotarsi di un sistema di sorveglianza "intelligente", provvisto anche di un sistema di captazione audio, che garantisse una veloce identificazione di possibili intrusioni dall'esterno da parte di persone non autorizzate.

Il Garante ha ritenuto che l'impianto di videosorveglianza intelligente fosse conforme ai princìpi di pertinenza, non eccedenza e proporzionalità (v. artt. 3 e 11 del Codice) poiché l'ubicazione isolata del sito, la sua notevole estensione e la posizione dell'area al di fuori delle zone in cui le forze dell'ordine svolgono la routinaria attività di pattugliamento, giustificavano l'adozione di sistemi di sicurezza che, consentendo una rilevazione di possibili intrusioni in tempi estremamente brevi, risultassero effettivamente in grado di prevenire accessi non autorizzati alla struttura e, quindi, riducessero significativamente il rischio di atti in grado di provocare gravi disservizi.

Invece, con specifico riferimento al connesso sistema di captazione audio, l'Autorità ha ritenuto che lo stesso non fosse conforme al richiamato principio di proporzionalità, potendo determinare un'ulteriore e non giustificata riduzione della sfera di riservatezza di chiunque si trovasse a transitare in prossimità di un'area già abbondantemente monitorata, per finalità di sicurezza, con un modernissimo sistema di videosorveglianza.

Pertanto, è stata accolta la richiesta di verifica preliminare limitatamente alla sola attività di videosorveglianza e non per il sistema di captazione audio.

È stata altresì accolta, con provvedimento del 15 marzo 2012 [doc. web n. 1893742], in sede di verifica preliminare, l'istanza presentata da una società operante tra altro nei settori del petrolio, del gas naturale e della petrolchimica, volta all'istallazione di due sistemi di videosorveglianza cd. "intelligente" presso due suoi siti produttivi, per finalità connesse alla tutela del patrimonio aziendale e della sicurezza dei lavoratori.

In particolare, l'Autorità ha considerato sia che le situazioni di rischio erano state espressamente acclarate a più riprese dagli organi istituzionalmente preposti, sia la ridotta efficacia delle protezioni e dei sistemi di sicurezza esistenti ed ha perciò ritenuto giustificata l'attivazione di un sistema di video-analisi a supporto dei dispositivi di ripresa che, consentendo una rilevazione automatica delle intrusioni, risultasse effettivamente in grado di prevenire accessi non autorizzati alla struttura, forieri di grave pericolo per la sicurezza dei siti in questione e l'incolumità del personale ivi impiegato.

È stata invece respinta, in sede di verifica preliminare, l'istanza di conservare sino a novanta giorni le immagini del sistema di videosorveglianza di una società che opera nella persona-

lizzazione e postalizzazione di tessere magnetiche ed a microprocessore, per applicazioni di sicurezza e sanitarie (carte di credito e, più in generale, carte di identificazione).

La richiesta era stata giustificata non solo con l'esigenza di rafforzare il livello di tutela della proprietà aziendale e di sicurezza, ma anche con la necessità di osservare concretamente i parametri fissati dai circuiti internazionali *MasterCard International* e *Visa International*, presso i quali l'azienda risultava certificata per la produzione di carte di credito.

Il Garante ha in contrario osservato, da un lato, che le "prescrizioni" impartite dagli enti certificatori risultavano "derogabili" in presenza di "restrizioni legali" all'utilizzo di sistemi di videosorveglianza; dall'altro, che non si erano mai verificate in concreto condotte criminose (verosimilmente anche in ragione delle altre numerose misure di sicurezza già approntate).

L'Autorità ha peraltro ricordato il consolidato orientamento giurisprudenziale che riconosce al datore di lavoro la possibilità, nel rispetto delle garanzie previste dall'ordinamento (in particolare, gli artt. 2, 3 e 6 della l. n. 300/1970), di adibire a mansioni di vigilanza e tutela del patrimonio aziendale anche propri dipendenti, a mezzo dei quali poter controllare l'attività di altri lavoratori per accertare eventuali comportamenti fraudolenti estranei alla prestazione lavorativa e rilevanti sull'integrità del patrimonio aziendale (provv. 21 marzo 2012 [doc. web n. 1893723]).

Si riferisce, infine, di una richiesta di verifica preliminare inoltrata da una società che gestisce un importante complesso museale con sede in Venezia, per l'allungamento dei tempi di conservazione delle immagini registrate dal sistema di videosorveglianza -rispetto a quelli indicati nel provvedimento generale adottato dal Garante in materia (provv. 8 aprile 2010 [doc. web n. 1712680])- giustificato dal pericolo di furti e di atti vandalici, in molti casi rilevabili solo a distanza di tempo, cui sarebbero state esposte numerose opere di inestimabile valore custodite all'interno del museo.

A seguito di tale richiesta, il Garante ha ritenuto sussistente il rischio paventato, considerate le dimensioni delle sale d'esposizione e il numero delle opere esposte e dei visitatori; ha quindi accolto la richiesta di allungamento dei tempi di conservazione delle immagini sino a due settimane, con successiva cancellazione automatica delle stesse (provv. 8 marzo 2012 [doc. web n. 1891026]).

14.5. BIOMETRIA

A seguito di due distinte segnalazioni, l'Autorità è stata chiamata a pronunciarsi sulla liceità del trattamento di dati biometrici effettuato presso due centri sportivi per finalità di accesso alle relative strutture e di gestione dei servizi offerti (provv.ti 16 febbraio 2012 [doc. web n. 1894570] e 29 marzo 2012 [doc. web n. 1891999]). Dagli accertamenti ispettivi espletati è emerso come non fosse stato nemmeno acquisito un libero consenso degli interessati rispetto allo specifico trattamento dei dati biometrici con conseguente violazione degli artt. 11, comma 1, lett. *a)* e 23, del Codice. Peraltro, a fronte della indimostrata insufficienza o non attuabilità di eventuali misure alternative alla rilevazione del dato biometrico, il trattamento è risultato vieppiù sproporzionato (art. 11, comma 1, lett. *d)*, del Codice) in ragione delle prescelte modalità di configurazione del sistema, preordinato alla conservazione centralizzata dei *template* in luogo della loro memorizzazione su dispositivi affidati esclusivamente agli interessati. In un caso, poi, il trattamento dei dati biometrici, che interessava anche alcuni lavoratori, è risultato altresì in violazione delle prescrizioni contenute nel provvedimento generale recante le linee-guida in materia (provv. 23 novembre 2006 [doc. web n. 1364099]). L'Autorità ha quindi vietato, nei confronti dei rispettivi titolari, l'ulteriore trattamento dei dati biometrici degli utenti.

Il Garante ha invece ammesso il trattamento dei dati biometrici dei passeggeri connesso all'installazione, presso i *gate* presenti in aeroporto, di un sistema di rilevazione delle loro impronte digitali volto a coniugare le esigenze di rigoroso accertamento dell'identità degli interessati con quelle di semplificazione e velocizzazione delle operazioni di imbarco cd. "*fast-boarding*" (provv. 4 ottobre 2012 [doc. web n. 2059743]).

Il trattamento -basato sulla conversione del rilievo dattiloscopico in un *template* memorizzato, unitamente ai dati identificativi dell'interessato, su una *smartcard* posta nell'esclusiva disponibilità di quest'ultimo e leggibile, attraverso l'utilizzo di tecnologia *Rfid*, solamente dal dispositivo a ciò preposto cd. "*reader*"-, sarebbe stato effettuato nel rispetto di rigorose misure di sicurezza a garanzia degli interessati e su base esclusivamente volontaria, previa acquisizione del libero consenso informato degli interessati. L'Autorità, nel valutare positivamente l'iniziativa (anche in ragione dei rigidi protocolli di sicurezza in ambito

aeroportuale previsti dalla normativa di settore), ha ritenuto che il trattamento così configurato non fosse illecito né sproporzionato. Nondimeno, fermo restando l'obbligo di notifica del trattamento (artt. 37 e ss. del Codice) e il rispetto delle previste misure di sicurezza (in particolare, la regola 25 dell'Allegato B. al Codice), è stato prescritto alla società di indicare chiaramente, nell'informativa da rendere all'utenza, le finalità del trattamento e la natura del conferimento dei dati, nonché di adottare una serie di accorgimenti volti a ridurre ulteriormente l'utilizzo di dati personali nell'ambito del servizio offerto.

Inoltre, con riguardo a due distinte verifiche preliminari (ai sensi dell'art. 17 del Codice) richieste da alcuni istituti di credito e da una *certification authority*, l'Autorità ha valutato il trattamento connesso all'utilizzo, nell'ambito del più ampio servizio di sottoscrizione dei documenti con firma digitale, di sistemi di autenticazione basati sulla rilevazione dei dati biometrici degli utenti in occasione delle operazioni allo sportello (provv. 31 gennaio 2013 [doc. web n. 2304808]). Tali sistemi, preordinati alla raccolta delle caratteristiche "comportamentali" degli interessati attraverso l'analisi di alcuni parametri (quali velocità, pressione, accelerazione, inclinazione) desumibili dall'apposizione della loro firma autografa su *tablet* a ciò dedicati, avrebbero garantito -attraverso la comparazione dei *template* acquisiti di volta in volta allo sportello con lo *specimen* di firma generato in occasione della registrazione al servizio- il rigoroso riconoscimento degli utenti (in osservanza, tra l'altro, degli specifici obblighi gravanti sugli istituti di credito e sui soggetti certificatori), riducendo conseguentemente i rischi connessi ad eventuali pratiche fraudolente (quali il furto di identità).

Il Garante, nel richiamare i pareri resi in materia dal Gruppo Art. 29 (WP 80 - 1° agosto 2003 [doc. web n. 1609419]; WP 193 - 27 aprile 2012 [doc. web n. 2375294]), ha sottolineato come il trattamento dei dati biometrici degli utenti risultasse effettivamente rispondente, nei casi esaminati, alle esigenze di rigoroso riconoscimento evidenziate dagli istanti, oltre che funzionale al contrasto di eventuali fenomeni fraudolenti e allo snellimento delle operazioni allo sportello; tanto, muovendo dall'ulteriore presupposto che, in entrambi i casi considerati, il trattamento sarebbe stato effettuato previa acquisizione del consenso informato degli interessati. Inoltre, sono risultate adeguate le modalità di configurazione del sistema e di gestione dei dati prescelte dagli istanti, come pure le misure di sicurezza indicate

a tutela dei dati biometrici oggetto di trattamento (artt. 31 e ss. del Codice). L'Autorità ha tuttavia prescritto, in un caso, alcune misure e accorgimenti, con particolare riferimento all'informativa da rendere agli interessati (art. 13 del Codice), all'acquisizione del loro consenso (art. 23 del Codice), ai tempi di conservazione dei dati (art. 11, comma 1, lett. *e)*, del Codice) e, infine, alla modifica della notificazione del trattamento (provv. 31 gennaio 2013 [doc. web n. 2311886]).

15. Il trasferimento dei dati all'estero

Nel periodo di riferimento l'attività del Garante si è svolta su differenti piani. Innanzitutto è proseguita l'analisi delle molteplici richieste di autorizzazione pervenute in materia di *Binding corporate rules (Bcr)* (norme vincolanti di impresa) e delle decisioni adottate dalla Commissione europea sull'adeguatezza delle normative di protezione dei dati di alcuni Paesi terzi (decisione relativa alla Repubblica orientale dell'Uruguay del 21 agosto 2012 e alla Nuova Zelanda del 19 dicembre 2012).

Quanto alle istanze concernenti l'impiego delle *Bcr*, sono state avviate istruttorie complesse, tuttora in corso, concernenti operazioni di trasferimento all'estero di dati effettuate da importanti gruppi multinazionali operanti in diversi settori economici; tali istruttorie sono frutto di procedure poste in essere a livello europeo, per lo più nell'ambito del cd. "accordo di mutua collaborazione" (cfr. Relazione 2009 p.189).

Altrettanto intensa, poi, è stata l'attività in materia di *standard contractual clauses*, con particolare riferimento anche a quanto evidenziato dal Garante italiano -in occasione delle attività di approfondimento condotte dal Gruppo Art. 29 con il documento WP 176 del 12 luglio 2010- riguardo ad alcuni quesiti formulati in vista dell'entrata in vigore della decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE.

Come già diffusamente descritto nelle precedenti Relazioni (v. Relazione 2009 p. 189 e Relazione 2010 p. 154) il Garante, con specifica autorizzazione (v. provv. 27 maggio 2010 [doc. web n. 1728496]), ha attuato nell'ordinamento italiano la Decisione della Commissione n. 2010/87/EU del 5 febbraio 2010, che ha sostituito il *set* di clausole contrattuali tipo "da titolare a responsabile" già esistente (Decisione della Commissione n. 2002/16/EC) con un nuovo schema che contiene una clausola cd. di "*subcontracting*", secondo cui l'importatore (in qualità di responsabile del trattamento) può affidare il trattamento (o una parte di esso) a un soggetto terzo (cd. "*sub-incaricato*"), che agisce anch'esso come responsabile.

A seguito di tale delibera, sono pervenuti a questa Autorità vari quesiti, di analogo tenore a quelli contenuti nel WP 176, volti a conoscere se sia possibile utilizzare il citato modello di

clausole contrattuali tipo anche nel caso in cui il responsabile, che affidi il trattamento ad un "*sub-incaricato*" ubicato in un Paese terzo che non assicuri un livello di protezione adeguato, sia stabilito nella Unione europea. Tali richieste sono state determinate dalla crescente diffusione di forme di affidamento di attività di trattamento a terzi (in particolare, a società di servizi, spesso stabilite nell'Unione europea) e dalla consequenziale esigenza del settore privato di disporre di strumenti comuni e di modalità uniformi da utilizzare nei casi in cui tale affidamento comporti un successivo trasferimento di dati personali verso Paesi terzi che non assicurino un livello di protezione adeguato.

Al riguardo, in questa prima fase, il Garante ha adottato un provvedimento (provv. 15 novembre 2012 [doc. web n. 2191156]) con il quale, tenuto conto di quanto previsto nel considerando 23 della citata Decisione n. 2010/87/UE e di quanto già accennato al riguardo nella menzionata autorizzazione dell'Autorità, ha prescritto al titolare del trattamento stabilito nel territorio dello Stato (esportatore) di conferire al responsabile stabilito nell'Unione europea che intenda affidare il trattamento dei dati ad un altro responsabile (importatore) stabilito nel Paese terzo che non assicuri un livello di protezione adeguato, un apposito mandato (ai sensi dell'art. 1704 c.c.), per la sottoscrizione delle clausole contrattuali tipo di cui all'allegato della Decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE.

La scelta di tale strumento da parte dell'Autorità, che lascia intatta la facoltà del titolare del trattamento di chiedere al Garante una specifica autorizzazione per trasferire i dati personali (ai sensi dell'art. 44, comma 1, lett. *a*), del Codice), è frutto anche del recepimento delle osservazioni e dei suggerimenti resi in tal senso dal Gruppo Art. 29 il quale, tra le possibili soluzioni, aveva ipotizzato l'utilizzazione dello schema contrattuale del mandato.

Infine, di rilievo è stato l'esame condotto dall'Autorità in ordine a due istanze -di analogo contenuto- avanzate da due società aventi sede in Italia ed operanti nel settore dell'offerta di prodotti assicurativi di risparmio e di cd. "*employee benefits*", volte ad ottenere un'autorizzazione al trasferimento di dati personali verso altre società, anch'esse titolari del trattamento, situate negli Stati Uniti.

In particolare, le istanze avevano ad oggetto il trasferimento dei dati personali relativi al personale per il perseguimento non solo delle finalità connesse alla gestione della forza

lavoro, ma anche per comunicazioni ed emergenze, per il compimento di operazioni commerciali e per attività di *compliance*, monitoraggio e pianificazione integrata svolte ordinariamente dalle società.

Dopo una complessa istruttoria, volta a valutare se il cd. "contratto di trasferimento" utilizzato dalle suddette società per il trasferimento dei dati all'estero contenesse adeguate garanzie per i diritti degli interessati, l'Autorità ha rilasciato le autorizzazioni richieste, nei limiti delle modalità e delle finalità indicate nel suddetto "contratto", riservandosi di controllare la liceità e la correttezza dei trasferimenti dei dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento (provv. 11 ottobre 2012 [doc. web n. 2111613]).

Per quanto riguarda la valutazione del Gruppo Art. 29 sull'adeguamento del livello di protezione dei dati personali nel Principato di Monaco, si fa rinvio al paragrafo 21.3..

16. Le libere professioni

16.1. Ordini professionali

Il Garante ha fornito numerosi chiarimenti in ordine alle modalità di trattamento ed al regime di conoscibilità dei dati personali degli iscritti agli ordini professionali. In particolare, ad un ordine che aveva effettuato una comunicazione al Garante, ai sensi degli artt. 19, comma 2, e 39 del Codice, per poter trasmettere a diversi soggetti i provvedimenti disciplinari assunti a carico di un iscritto, l'Autorità ha precisato che gli ordini e i collegi professionali possono comunicare a terzi, e diffondere, anche mediante reti di comunicazione elettronica, i dati diversi da quelli sensibili e giudiziari, che, secondo le disposizioni di settore, devono essere inseriti nei rispettivi albi (cfr. artt. 18, 19 e 61 del Codice). L'Ufficio ha evidenziato che, nel rispetto dei princìpi di pertinenza, non eccedenza e proporzionalità dei dati, il Codice consente di menzionare l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio delle professione, purché il trattamento riguardi informazioni corrette, complete ed aggiornate (nota 22 agosto 2011).

In relazione ad un quesito circa il regime di conoscibilità dell'indirizzo di posta elettronica certificata degli avvocati iscritti all'albo, l'Ufficio, nel ribadire i presupposti suddetti, ha evidenziato che nell'albo degli avvocati deve essere indicato, oltre al codice fiscale, anche l'indirizzo di posta elettronica certificata (cfr. art. 16 r.d. 27 novembre 1933, n. 1578 e successive modificazioni, recante "Ordinamento delle professioni di avvocato e procuratore") (nota 23 maggio 2011).

È giunto inoltre all'Autorità un reclamo relativo ad un collegio professionale dei periti industriali che, nell'ambito della campagna elettorale per le elezioni di un organo consiliare, aveva diffuso sul proprio sito internet istituzionale dati giudiziari relativi al reclamante e ad altri professionisti, iscritti, per altro, ad un altro collegio. Al riguardo, l'Autorità ha ribadito che il collegio, quale soggetto pubblico, può trattare dati giudiziari solo sulla base di idonea previsione normativa (v. artt. 20 e 21 del Codice).

In tale quadro il Ministero della giustizia ha adottato, in conformità al parere espresso dal Garante il 7 dicembre 2006 [doc. web n. 1370395], lo schema tipo di regolamento per il

trattamento dei dati sensibili e giudiziari da parte degli organismi professionali sottoposti alla sua vigilanza che, con riferimento al trattamento dei dati sensibili e giudiziari "*indispensabili allo svolgimento delle elezioni e alla gestione dei componenti degli organi elettivi del Consiglio/collegio*", ammette la diffusione "*limitatamente ai risultati elettorali*" (scheda n. 4). Rilevata l'illiceità della predetta diffusione, l'Autorità ha quindi vietato al collegio professionale di diffondere ulteriormente i dati giudiziari contenuti nei predetti atti (artt. 143, comma 1, lett. *c)*, e 154, comma 1, lett. *d)*, del Codice). L'Ufficio ha, infine, disposto gli opportuni accertamenti per l'eventuale applicazione della sanzione amministrativa conseguente alla violazione del divieto di diffusione (art. 162, comma 2-*bis*, del Codice) (provv. 17 gennaio 2013 [doc. web n. 2315622]).

Un iscritto all'ordine dei commercialisti ha lamentato, da parte del relativo ordine, la pubblicazione sull'albo dell'indirizzo completo relativo alla residenza anagrafica di ogni singolo iscritto. Al riguardo, in base alla normativa di settore, il predetto albo deve contenere, per ogni iscritto, tra l'altro, "*il cognome, il nome, la data ed il luogo di nascita, la residenza e l'indirizzo (anche telematico se posseduto) degli studi professionali*" (art. 34 del d.lgs. 28 giugno 2005, n. 139). Per residenza deve necessariamente intendersi l'indirizzo completo di residenza anagrafica, rilevante sia ai fini dell'iscrizione e della permanenza nell'albo, anche in considerazione dei poteri di vigilanza disciplinare spettanti all'ordine, sia ai fini civilistici e processuali. Per tali ragioni, l'Ufficio ha ritenuto di non dover promuovere iniziative per l'adozione di specifici provvedimenti da parte del Collegio (nota 5 giugno 2012).

16.2. ORGANISMI DI MEDIAZIONE

Il d.lgs. 4 marzo 2010, n. 28 disciplina e configura come obbligatoria -in termini giudicati incostituzionali dalla Corte costituzionale con sentenza n. 272 del 6 dicembre 2012- la mediazione finalizzata alla conciliazione delle controversie civili e commerciali per chi intenda esercitare in giudizio un'azione nelle materie ivi previste. La mediazione è volta ad assistere due o più soggetti sia nella ricerca di un accordo amichevole per la composizione di una controversia, sia nella formulazione di una proposta per la risoluzione della stessa. Il procedimento è gestito da organismi di mediazione, costituiti da enti

pubblici o privati che, all'atto della presentazione della domanda di mediazione, designano un mediatore o più mediatori ausiliari.

L'Autorità è intervenuta al fine di assicurare che, nell'ambito di tale procedimento, siano rispettate tutte le garanzie previste dalla normativa di settore a tutela, in particolare, dei dati sensibili (si pensi, ad es., ai procedimenti inerenti il risarcimento del danno da responsabilità medica e da diffamazione) e giudiziari (quali i dati relativi a sentenze di condanna in base alle quali si può richiedere il risarcimento del danno) riferiti alle parti della mediazione e ad altri soggetti eventualmente coinvolti nel procedimento stesso.

In tale quadro e con specifico riferimento ai soggetti pubblici che intendano costituire un organismo di mediazione, con apposito provvedimento del Garante, in collaborazione con il Ministero della giustizia, sono stati identificati i tipi di dati che possono essere trattati e le operazioni eseguibili per il perseguimento della rilevante finalità di far valere il diritto di difesa (art. 71, comma 1, lett. *b),* del Codice; provv. 21 aprile 2011 [doc. web n. 1809039]). Gli enti pubblici che intendano costituire un organismo di mediazione, nell'adeguare il proprio regolamento per il trattamento dei dati sensibili e giudiziari -che ciascun soggetto pubblico deve avere adottato ai sensi dell'art. 20 del Codice- possono, quindi, avvalersi del documento allegato al predetto provvedimento, senza richiedere all'Autorità un parere specifico per poter trattare dati sensibili e giudiziari per l'attività degli organismi di mediazione (artt. 20, comma 2, e 21, comma 2, del Codice).

Nell'ipotesi in cui i suddetti organismi siano costituiti da soggetti privati, il Garante ha autorizzato il trattamento di dati sensibili delle parti coinvolte nell'attività di mediazione finalizzata alla conciliazione delle controversie civili e commerciali con un provvedimento di carattere generale, con il quale sono stati stabiliti i princìpi e le misure per il corretto trattamento di tali dati (provv. 21 aprile 2011 [doc. web n. 1808658]).

Gli organismi di mediazione pubblici e privati, il Ministero della giustizia e gli enti di formazione di cui all'art. 16, comma 5, del d.lgs. 4 marzo 2010, n. 28 e successive modificazioni e integrazioni, e all'art. 1, comma 1, lett. *n),* del d.m. n. 180/2010, sono stati autorizzati, inoltre, sempre con un provvedimento di natura generale, a trattare i dati giudiziari per la verifica dei requisiti di onorabilità di soci, associati, amministratori e

rappresentanti degli organismi di mediazione e degli enti di formazione di natura privata, nonché dei singoli mediatori (provv. 21 aprile 2011 [doc. web n. 1808676]).

I titolari dei trattamenti che rientrano nell'ambito di applicazione di entrambe le autorizzazioni generali -efficaci fino al 30 giugno 2012- e che intendano effettuare un trattamento di dati sensibili e/o giudiziari, conforme alle prescrizioni in esse contenute, non sono tenuti a presentare una specifica richiesta di autorizzazione a questa Autorità.

16.3. ATTIVITÀ FORENSE E INVESTIGATIVA

Nel corso del 2012 sono pervenute all'Autorità numerose segnalazioni relative al trattamento di dati personali nell'ambito dell'attività forense e investigativa, effettuato "*per far valere o difendere in sede giudiziaria un diritto*".

Utilizzo dei dati depositati in giudizio

Nel fornire riscontro a un quesito posto da un avvocato riguardante la legittimità dell'utilizzo di dati personali depositati dalla controparte in giudizio, il Garante ha chiarito che per lo svolgimento di indagini difensive di cui alla l. n. 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria (artt. 13, comma 5, lett. *b)* e 24, comma 1, lett. *f),* del Codice), l'informativa all'interessato e il suo consenso non sono richiesti, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (nota 2 aprile 2012).

Comunicazione dei dati a terzi

A diversa conclusione il Garante è giunto riguardo a una segnalazione con cui l'interessata, parte in un procedimento giudiziale di separazione, aveva contestato la condotta dell'avvocato del coniuge per aver trasmesso ad una struttura alberghiera, insieme a una richiesta di informazioni concernente l'interessata e la figlia, anche la copia integrale del ricorso in appello, contenente dati sensibili dell'interessata medesima. Non risultando la comunicazione di dati necessaria a far valere o difendere un diritto in sede giudiziaria, l'Autorità ha ritenuto il trattamento non conforme agli artt. 13, comma 5, lett. *b)* e 24, comma 1, lett. *f),* del Codice, avendo comportato una comunicazione di dati anche sensibili dell'interessata a soggetto non legittimato a conoscerli senza il consenso della medesima. Poiché il trattamento aveva ormai esaurito i suoi effetti, non è stato adottato alcun provvedimento prescrittivo o inibitorio ai sensi dell'art. 143, comma 1, del Codice (artt. 12, comma 4 e 14, comma 2, del Regolamento

n. 1/2007 del 14 dicembre 2007), salva la valutazione da parte dell'Autorità della ricorrenza di violazioni amministrative (nota 6 giugno 2012).

L'Autorità ha deciso in maniera analoga una segnalazione concernente il trattamento svolto dall'*ex* avvocato del segnalante, parte in un procedimento giudiziale di separazione, che aveva comunicato al legale del coniuge non solo la rinuncia al mandato, ma anche la notula delle prestazioni fornite al segnalante, in tal modo effettuando una comunicazione di dati personali a soggetto non legittimato a conoscerli senza il consenso dell'interessato (nota 19 settembre 2012).

In un'altra segnalazione l'interessato lamentava di aver ricevuto una raccomandata con avviso di ricevimento recante sulla busta anche il suo *status* di "fallito in proprio" e "legale rappresentante di una società fallita".

Il Garante ha ritenuto che l'indicazione dello *status* di fallito sulla busta risultasse eccedente (ai sensi dell'art. 11, lett. *d),* del Codice) rispetto alla finalità adottata dall'avvocato mittente di assicurare la presenza dell'interessato all'udienza fissata per l'approvazione del rendiconto di gestione, secondo quanto previsto dall'art. 116 della legge fallimentare e ha pertanto invitato il professionista a conformare pienamente le operazioni di trattamento alle disposizioni del Codice, evitando il ripetersi di episodi analoghi (nota 9 febbraio 2012).

In un altro caso, un pubblico dipendente aveva lamentato l'invio, da parte di un'avvocatura distrettuale dello Stato, di una sentenza di un Tar relativa ad una controversia tra il segnalante e l'amministrazione sua datrice di lavoro e contenente dati sensibili dell'istante, non all'ufficio territoriale dove l'esponente prestava servizio, bensì all'ufficio di una circoscrizione territoriale diversa. Nel fornire riscontro, il Garante ha rappresentato che la comunicazione dei dati sensibili effettuata ad un ufficio diverso da quello legittimato a conoscerli, risultava non conforme a quanto prescritto dall'art. 20 del Codice che ammette il trattamento dei dati sensibili da parte di soggetti pubblici.

Poiché il trattamento aveva ormai esaurito i suoi effetti, non si è proceduto all'adozione di un provvedimento prescrittivo o inibitorio ai sensi dell'art. 143, comma 1, del Codice (artt. 12, comma 4 e 14, comma 2, del Regolamento n. 1/2007 del 14 dicembre 2007), salva la valutazione da parte dell'Autorità della ricorrenza di violazioni amministrative (nota 22 marzo 2012).

Un interessato ha lamentato che l'avvocato della sua *ex* coniuge aveva inviato una diffida diretta nei suoi confronti, contenente informazioni riservate di carattere patrimoniale e familiare, al legale che lo aveva assistito nel corso del procedimento per la cessazione degli effetti civili del matrimonio, il cui mandato, a suo dire, si era esaurito con la definizione del procedimento.

Invitato a fornire chiarimenti, l'avvocato della donna, consapevole delle sanzioni penali previste in caso di inosservanza dell'art. 168 del Codice, ha dichiarato che l'intimazione aveva ad oggetto l'attuazione degli obblighi anche economici fissati dalla sentenza di divorzio e che il destinatario risultava essere ancora il legale di fiducia del segnalante. Sulla scorta anche della deliberazione del competente consiglio dell'ordine degli avvocati, che ha archiviato la segnalazione, l'Autorità non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali (nota 5 ottobre 2012).

Diffusione di dati

È stata lamentata la divulgazione da parte di un avvocato, tramite pubblicazione su un sito internet, di un atto prodotto in giudizio dall'interessato e relativo ad un procedimento giudiziale in corso, riguardante anche l'avvocato suddetto. Dall'istruttoria è risultato che la pubblicazione rientrava tra i trattamenti finalizzati alla manifestazione del pensiero, che possono essere effettuati anche senza il consenso dell'interessato rispettando i limiti del diritto di cronaca e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, commi 2 e 3, del Codice). Il documento pubblicato riguardava, infatti, un giudizio che aveva assunto un rilevante interesse pubblico non solo nell'ambito professionale, essendo stato trattato anche da organi di stampa; e non era risultato violato il principio di essenzialità dell'informazione, in quanto l'atto pubblicato non conteneva dati o elementi da ritenersi non essenziali rispetto alla sottesa vicenda di pubblico interesse. Il Garante non ha, pertanto, ravvisato violazioni della disciplina in materia di protezione dei dati personali (nota 26 luglio 2012).

Accesso agli atti amministrativi

Con riferimento ad un quesito presentato da un avvocato relativamente alle modalità attraverso cui è consentito ottenere da un istituto pubblico notizie relative alla posizione lavorativa di un debitore di una sua assistita, il Garante ha ricordato che in tema di accesso agli atti amministrativi il Codice sancisce che i presupposti, le modalità, i limiti e la tutela

giurisdizionale in materia di accesso restano disciplinati dalla l. 7 agosto 1990, n. 241 (artt. 59 e 60 del Codice). Nel caso di specie, poiché l'istanza era stata respinta, il Garante ha evidenziato la possibilità di presentare ricorso al tribunale amministrativo regionale ovvero chiedere alla commissione per l'accesso ai documenti amministrativi di riesaminare la determinazione, come prescritto dall'art. 25 della l. n. 241/1990, salvi i poteri istruttori del giudice competente nella causa in corso (nota 17 ottobre 2012).

Accesso per finalità di difesa a dati detenuti da terzi

Il Garante ha in più occasioni chiarito la posizione dei soggetti che detengono per legge o per contratto dati personali di terzi rispetto a richieste di accesso presentate da avvocati o investigatori privati "*per far valere o difendere in sede giudiziaria un diritto*".

In un caso, l'interessata aveva posto all'attenzione dell'Autorità una richiesta di informazioni presentata ad una società di abbigliamento volta a conoscere, in particolare, se un debitore dell'interessata risultasse essere dipendente della società che forniva la vigilanza presso la detta società di abbigliamento. Al riguardo, il Garante ha evidenziato che la disciplina in materia di protezione dei dati personali, pur esonerando chi intende raccogliere dati personali presso terzi "*per far valere o difendere un diritto in sede giudiziaria*" dal fornire l'informativa all'interessato e acquisire il suo consenso (artt. 13, comma 5, lett. *b)* e art. 24, comma 1, lett. *f),* del Codice), non pone a carico del soggetto destinatario della richiesta l'obbligo di fornire informazioni. Tale soggetto resta invece tenuto, in qualità di titolare del trattamento, a rispettare la disciplina in materia di protezione dei dati personali e a valutare l'opportunità e la liceità di rilasciare informazioni concernenti soggetti terzi (nota 13 febbraio 2012).

In un'analoga vicenda, un avvocato aveva contestato il rigetto, giustificato da motivi di *privacy*, delle richieste di informazioni presentate ad alcune compagnie telefoniche concernenti le intestazioni di numeri telefonici di utenze fisse e mobili relative ad atti d'indagine e procedimenti penali in corso. Anche in tale vicenda, è stato evidenziato che il Codice non pone a carico dei titolari del trattamento alcun obbligo a comunicare, ancorché a soggetti qualificati, i dati personali richiesti, trattandosi semmai di una facoltà da esercitare tenendo conto delle garanzie che l'ordinamento giuridico appresta per gli interessati. A tal fine, come chiarito nel provvedimento del 23 maggio 2001 [doc. web n. 39821] "*il titolare del trattamento, oltre a valutare l'effettiva necessità della comunicazione ai fini dell'esercizio del diritto*

di difesa, deve verificare che la natura dei dati, il contesto in cui essi sono trattati e, in particolare, il rapporto giuridico che lega il titolare medesimo all'interessato permetta di esercitare tale facoltà senza violare obblighi nascenti dalla legge o da un rapporto contrattuale" (nota 28 maggio 2012).

Accesso ad atti di pubbliche amministrazioni per svolgere indagini difensive

Un avvocato aveva contestato il rifiuto opposto da un'azienda ospedaliera ad un'istanza di estrazione di copia di alcuni documenti relativi ad una signora, ritenuti necessari per la difesa in giudizio del suo assistito, destinatario di un avviso di conclusioni delle indagini preliminari nell'ambito di un procedimento penale. Al riguardo, il Garante ha ricordato che l'art. 391-*quater* c.p.p. prevede che, ai fini delle indagini difensive, il difensore può richiedere i documenti in possesso della pubblica amministrazione ed estrarne copia a sue spese, con istanza rivolta all'amministrazione che ha formato il documento o lo detiene stabilmente, e che "*in caso di rifiuto da parte della pubblica amministrazione si applicano le disposizioni degli artt. 367 e 368*" (comma 3). Tali disposizioni hanno introdotto un mezzo di tutela demandato all'autorità giudiziaria tenuta a valutare l'istanza anche sotto il profilo del rispetto dei princìpi del Codice, con specifico riferimento all'art. 71 (v. Consiglio di Stato, sez. IV, 26.4.2007, n. 1896; Tar Lombardia, sez. I, 17.10.2006, n. 2013). Il Garante ha dichiarato, pertanto, la propria incompetenza sulla vicenda (nota 13 marzo 2012).

La disciplina di cui all'art. 391-*quater* c.p.p. è stata richiamata anche in un caso in cui alcuni legali avevano chiesto alla polizia stradale l'ostensione di verbali di violazioni al codice della strada (nota 5 settembre 2012).

Accesso ai tabulati telefonici per svolgere indagini difensive

Analogamente, il Garante ha dichiarato la propria incompetenza con riferimento alla segnalazione di un avvocato che, in qualità di difensore di una persona coinvolta in un procedimento penale, aveva lamentato il rifiuto opposto da una società di telefonia all'istanza volta ad acquisire copia dei tabulati telefonici nonché degli sms relativi all'utenza intestata alla sua assistita, con specifico riferimento ai tabulati telefonici in entrata, ai sensi dell'art. 8, comma 2, lett. *f),* del Codice. In particolare, l'Autorità ha ricordato che il difensore può richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391-*quater* c.p.p., sopra riportate (nota 6 dicembre 2012).

Accesso a cartelle cliniche per svolgere indagini difensive

Con riferimento all'istanza proposta al Garante ai sensi dell'art. 26 del Codice, di autorizzazione al trattamento dei dati sensibili avanzata da un avvocato per ottenere la visione

ed il rilascio da parte di un'azienda sanitaria provinciale di documentazione medico-sanitaria relativa ad una persona, ai fini dello svolgimento delle investigazioni difensive nell'ambito del processo penale nel quale l'assistito dell'avvocato risultava imputato, l'Autorità ha evidenziato che il Garante aveva già previsto tale fattispecie nell'autorizzazione n. 4/2011 al trattamento dei dati sensibili da parte di liberi professionisti (provv. 24 giugno 2011 [doc. web n. 1822597]) e che, nell'ipotesi prospettata, le condizioni per raccogliere, in tutto o in parte, eventuali richieste di presa visione o di rilascio di copia della cartella clinica da parte di soggetti diversi dall'interessato sono stabilite dall'art. 92 del Codice (nota 14 maggio 2012).

In un'analoga vicenda, una casa di cura aveva chiesto il parere del Garante sulla condotta da osservare a fronte della richiesta di accesso a dati di natura sanitaria contenuti in una cartella clinica, avanzata da alcuni avvocati al fine dichiarato di difendere in giudizio un loro assistito in un procedimento penale. Nel ricordare quanto disposto dall'art. 92 del Codice, il Garante ha evidenziato che spetta alla casa di cura, previa assunzione di informazioni certe sulla natura e consistenza dei diritti contrapposti nel caso specifico, effettuare il bilanciamento dei medesimi, onde determinare se quello che si intende tutelare con la richiesta di accesso ai documenti amministrativi sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (nota 15 ottobre 2012).

Custodia dei dati contenuti nei fascicoli da parte di studi legali

In una segnalazione l'interessato ha rappresentato che il suo *ex* avvocato, al momento di restituire fascicoli e documenti per cessato mandato, aveva dichiarato che parte di tale documentazione era andata distrutta in occasione di un allagamento dello studio, per il quale il segnalante aveva presentato denuncia all'Arma dei Carabinieri.

Sulla base degli elementi forniti dal professionista, che ha prodotto copia del decreto con il quale il gip del Tribunale di Genova aveva archiviato la denuncia del segnalante dal quale emergeva che nello studio del legale si era in effetti verificato un sinistro di natura alluvionale dovuto a fattori eccezionali e non imputabile alla mancata diligenza del professionista nella custodia dei fascicoli, il Garante non ha ravvisato violazioni della disciplina in materia di protezione dei dati, in particolare a quelle sulle misure di sicurezza (artt. 31 e ss. del Codice) (nota 28 giugno 2012).

Produzione di documenti in giudizio

Con riferimento specifico alla produzione documentale in sede giudiziaria il Garante, richiamando il proprio orientamento in materia (provv. 23 settembre 2010 [doc. web n. 1756065]; provv. 4 novembre 2010 [doc. web n. 1770943]; provv. 17 novembre 2010 [doc. web n. 1779765]), ha confermato che spetta al giudice adito, ove ritualmente richiesto, valutare la liceità del trattamento dei dati personali (art. 160, comma 6, del Codice). In diversi casi, dunque, il Garante ha dichiarato la propria incompetenza a valutare l'eventuale illiceità di tale trattamento, fatte salve le eventuali responsabilità di soggetti terzi (quali gli istituti di credito) per l'accertata e illecita comunicazione di dati personali successivamente prodotti in giudizio (*ex multis*, note 16 gennaio, 1° marzo, 28 maggio, 15 ottobre 2012).

Trattamento di dati personali da parte di investigatori privati

In risposta al quesito di un investigatore privato, concernente la legittimità di mancati riscontri da parte di strutture sanitarie a richieste effettuate per conto di compagnie di assicurazione in merito alla conformità al vero di certificati medici di pronto soccorso prodotti dalle parti di sinistri assicurativi, il Garante ha evidenziato che la conferma fornita ad un soggetto qualificato dell'autenticità o meno di un certificato non implica alcuna comunicazione di dati sensibili, attenendo invece all'esclusiva veridicità del certificato stesso; tanto più se la struttura sanitaria rappresenti all'investigatore che il certificato non sia conforme al vero, nel qual caso non si verificherebbe alcun trattamento di dati personali. La disciplina in materia di protezione dei dati non vieta né d'altra parte obbliga la struttura sanitaria a dare conto dell'autenticità o meno di un certificato medico. Assume pertanto rilievo la veste qualificata del richiedente desumibile dall'eventuale e documentata attività finalizzata all'accertamento di comportamenti fraudolenti di soggetti coinvolti in sinistri assicurativi, svolta nel pieno rispetto della disciplina di settore (con particolare riferimento all'incarico ricevuto) e della normativa in materia di protezione dei dati personali, alla luce altresì dell'autorizzazione del Garante n. 6/2011 (provv. 24 giugno 2011 [doc. web n. 1822629]) e del "Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive" del 6 novembre 2008 (in G.U. 24 novembre 2008, n. 275 [doc. web n. 1565171]) (nota 17 gennaio 2012).

Richiamando l'art. 135 del Codice e il citato codice di deontologia, con riferimento ad una segnalazione riguardante una persona assoggettata ad attività di investigazione privata, il

Garante ha ricordato che il Codice consente il trattamento dei dati personali per far valere o difendere un diritto in sede giudiziaria, per il quale non è richiesta né l'informativa all'interessato, né il suo consenso. Inoltre, l'attuale normativa consente e disciplina il trattamento dei dati personali da parte dei liberi professionisti o dei soggetti che esercitano un'attività di investigazione privata autorizzata in conformità alla legge, ai fini dello svolgimento di indagini difensive o per far valere o difendere un diritto in sede giudiziaria (nota 8 ottobre 2012).

In un'altra vicenda, il Garante ha invitato un'agenzia investigativa, che aveva informato l'Autorità di far uso di apparecchiature tipo *Gps* con una comunicazione incompleta e carente di diversi elementi, a provvedere alla prescritta notifica, di cui agli artt. 37 e 38 del Codice, seguendo la procedura descritta nel sito internet del Garante (nota 6 dicembre 2012).

17. Il registro dei trattamenti

In attuazione di una specifica previsione del Codice (art. 154, comma 1) il Garante cura la tenuta del Registro dei trattamenti, un registro *online* formato sulla base delle notificazioni ricevute, effettuabili esclusivamente attraverso una procedura telematica. La consultazione del Registro stesso, consentita a chiunque e gratuita (art. 37, comma 4, del Codice), ha luogo per via telematica attraverso l'accesso ad una sezione del sito web dell'Autorità ora denominata "servizi *online*". Agli utenti è consentita la stampa integrale delle notificazioni.

L'obbligo di notificazione al Garante, ossia di comunicare in via preventiva l'intenzione di procedere al trattamento o di modificarne o cessarne uno in corso, sorge in capo al titolare del trattamento dei dati personali ove ricorra uno dei casi previsti dall'art. 37 del Codice e non si versi in una delle ipotesi di esonero individuate dall'Autorità con proprie deliberazioni (v. Relazione 2004 p. 109, provv. 31 marzo 2004 [doc. web n. 852561]; nota 23 aprile 2004 [doc. web n. 993385]; nota 26 aprile 2004 [doc. web n. 996680]; provv. 24 giugno 2011 [doc. web n. 1823225]). La notificazione consiste in una dichiarazione formale compilata direttamente sul computer dell'utente seguendo l'apposita procedura disponibile sul sito dell'Autorità; le modalità di compilazione del modello informatico e i suoi contenuti sono stati semplificati a decorrere dal 2008 (provv. 22 ottobre 2008 [doc. web n. 1571196]).

Il più recente provvedimento di esonero, del 2011, ha riguardato i trattamenti di dati genetici da parte degli organismi di mediazione nell'ambito dell'attività finalizzata alla conciliazione delle controversie civili e commerciali (provv. 24 giugno 2011 [doc. web n. 1823225]).

L'assistenza nei confronti dei titolari dei trattamenti è assicurata non solo attraverso un servizio di messaggistica automatica generato dalla procedura telematica di notificazione, ma anche grazie al supporto tecnico ed amministrativo offerto dal personale addetto, sia via e-mail, sia telefonicamente. Il Dipartimento ha garantito una rapida soluzione dei problemi più comuni segnalati dagli utenti mediante un controllo in tempo reale della procedura.

Nel 2012 gli utenti hanno consultato il Registro con una media giornaliera di oltre 70 accessi e punte superiori ai 200.

Con riguardo al numero delle notificazioni presentate, l'anno 2012 presenta un andamento discontinuo. In particolare, nel primo e nel secondo trimestre dell'anno si registra un decremento delle notificazioni rispetto ai corrispondenti trimestri del 2011, verosimilmente in connessione con la dinamica negativa del ciclo economico in tali periodi (nel primo e secondo trimestre del 2012 si registra, infatti, un decremento del Pil rispettivamente dello 0,9% e dello 0,7%). Nella seconda metà del 2012, che registra una flessione del Pil di minore entità, si verifica invece, un incremento del numero delle notificazioni rispetto ai corrispondenti ultimi due trimestri del 2011, con una tendenza alla crescita che parrebbe confermata nel mese di gennaio 2013, che ha visto il maggior numero di notificazioni nel mese di gennaio dal 2007.

I dati percentuali relativi alla tipologia dei trattamenti notificati nel 2012 confermano nel loro insieme, con limitati scostamenti, le tendenze del periodo 2004-2011. I trattamenti volti a definire il profilo e la personalità dell'interessato tramite l'ausilio di strumenti elettronici (28%), di dati idonei a rivelare lo stato di salute e la vita sessuale (22%) e quelli relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (19%), coprono da soli quasi il 70% di tutti i trattamenti notificati.

In merito infine alla distribuzione geografica dei titolari, vale quanto già evidenziato negli anni precedenti. Il nord del Paese esprime da solo il 57% dei notificanti. Tale decisa prevalenza potrebbe essere ascrivibile a diversità economiche di natura strutturale.

Va rilevato poi, che nel 2012 le notificazioni presentate direttamente dai titolari, come nel 2011, hanno superato in numero assoluto quelle presentate tramite intermediario. Tale tendenza è da attribuirsi al sempre più diffuso utilizzo della firma digitale ed indica, più in generale, una maggiore confidenza dei cittadini con le procedure telematiche nei rapporti con le autorità pubbliche.

Si conferma, infine, come già prospettato lo scorso anno, che la disciplina della materia potrebbe costituire oggetto di modifiche, nell'ambito della proposta, presentata dalla Commissione europea il 25 gennaio 2012, di un regolamento generale sulla protezione dei dati personali destinato a sostituire la Direttiva n. 95/46/CE. Nel testo si ipotizza l'abolizione dell'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito

da quello di nominare un *data protection officer* (incaricato della protezione dati, secondo la terminologia della Direttiva n. 95/46/CE) per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti (per dettagli sull'*iter* delle proposte modifiche v. *infra* par. 21.).

18. La trattazione dei ricorsi

18.1. Profili generali

Il paragrafo dedicato alla trattazione dei ricorsi costituisce, tradizionalmente, occasione di riflessione trasversale che, attraverso la lente del più formale e strutturato strumento di tutela previsto dal Codice, offre un variegato panorama sia sui temi consolidati affrontati dal Garante e sul complessivo svolgimento della sua attività, sia su vicende che pongono in luce aspetti innovativi della protezione dei dati personali. Al tempo stesso, l'esame della tipologia dei ricorsi consente di "tastare il polso" al modo in cui la legge sulla *privacy* è concretamente percepita e a come la stessa si raccorda alle più ampie e complesse problematiche economiche e sociali.

Da questo punto di vista è oggi facile leggere tra le righe di tanti ricorsi il riflesso dell'acuta crisi economica che stiamo attraversando. Non a caso negli ultimi anni è stato molto elevato il numero di procedimenti che ha interessato l'ambito economico-finanziario latamente inteso. In un quadro di difficoltà economiche, di restrizione del credito, di contraccolpi e perdite indotti dalla cd. "finanza creativa" e dalla sottoscrizione di prodotti finanziari strutturati, molti interessati hanno utilizzato l'esercizio dei diritti di cui all'art. 7 del Codice (e in particolare il diritto di accesso ai dati personali) per ricostruire, ad esempio, il quadro contabile degli investimenti effettuati, per verificarne le condizioni di liceità del trattamento (presenza di informative e corretta acquisizione dei necessari consensi), per documentare la successione delle operazioni effettuate e dei risultati con le stesse conseguiti. Per altro verso, l'aumento delle sofferenze bancarie e la correlata necessità di verificare attentamente l'affidabilità e la solvibilità dei soggetti richiedenti credito ha portato con sé un inevitabile contenzioso in ordine all'azione (e al conseguente trattamento dei dati) degli organismi pubblici e privati che agiscono nel settore della cd. "centralizzazione del rischio creditizio" (Centrale dei rischi della Banca d'Italia e Sistemi privati di informazione creditizia) o che comunque registrano, sulla base delle risultanze degli archivi pubblici, altri indici di "difficoltà" delle imprese (ad es., le società che operano nel settore delle cd. "informazioni commerciali") o la violazione di specifiche disposizioni normative (ad es., la Centrale

d'allarme interbancaria in rapporto alle violazioni delle norme in materia di corretto utilizzo degli assegni bancari e delle carte di pagamento).

Se i ricorsi proposti nei confronti di banche, società finanziarie, organismi di centralizzazione delle informazioni creditizie, rappresentano uno dei volti della crisi in atto, un aspetto altrettanto significativo è rappresentato dall'elevato numero di procedimenti concernenti controversie in materia di lavoro. Le tensioni che caratterizzano il mercato del lavoro, il deteriorarsi delle relazioni sindacali all'interno di grandi imprese in crisi, i problemi legati agli esuberi di personale, le nuove politiche salariali che valorizzano le valutazioni sulla qualità e quantità dell'impegno professionale, sono tutti elementi che fanno da sfondo alle controversie in materia di utilizzo dei dati personali dei lavoratori. Ciò, con riferimento sia a rituali richieste di accesso, sia a più complessi procedimenti incentrati sulla contestazione di controlli (effettuati a mezzo di strumenti elettronici oppure con l'ausilio di investigatori privati) mirati a verificare la lealtà e la regolarità della prestazione lavorativa.

In questa carrellata forzatamente sommaria non può mancare un richiamo ai diversi procedimenti relativi al trattamento dei dati in ambito giornalistico, settore che pure evidenzia la prepotente avanzata delle tecnologie digitali. Sempre meno numerosi sono, infatti, i casi che riguardano la carta stampata, mentre sono in costante ascesa le problematiche concernenti il giornalismo *online* (cfr. *infra* par. 18.5.) e la conservazione digitale delle notizie.

18.2. UNO SGUARDO AI DATI STATISTICI

Al di là dei temi emergenti sopra segnalati, l'esame della tabella numerica riassuntiva dell'attività svolta nell'anno 2012 (cfr. *infra* par. 24 tab. 1.) consente qualche interessante rilievo e fornisce indicazioni sull'evoluzione della protezione dei dati in Italia.

Ancora una volta balza agli occhi la ulteriore progressiva diminuzione del numero di decisioni adottate (233 provvedimenti rispetto ai 257 del 2011), oggetto nelle precedenti relazioni di considerazioni che in buona misura si ribadiscono. Vale la pena di osservare qui che tali considerazioni, unitamente alla vastità dell'ambito di applicazione dei provvedimenti di carattere generale -adottati tra l'altro per fornire adeguata, se non esaustiva, risposta a problematiche ricorrenti- e ad un fisiologico rallentamento dell'attività per l'avvicendamento

dei componenti il Collegio sono riferibili anche alla diminuzione del numero complessivo dei provvedimenti collegiali che si riscontra nel 2012 (440 rispetto ai 538 del 2011).

Sicuramente è terminata la fase iniziale nella quale il ricorso era, di fatto, l'unico strumento effettivo di tutela dei nuovi diritti riconosciuti in materia di protezione dei dati personali. Ciò, a fronte di una scarsa conoscenza della normativa e di una diffusa difficoltà da parte di imprese e pubbliche amministrazioni a corrispondere in modo pertinente e tempestivo alle richieste, già numerose, degli interessati: quasi a confermare che la consapevolezza (magari ancora ingenua e confusa) delle nuove posizioni giuridiche da tutelare era più diffusa fra gli interessati che non fra le burocrazie pubbliche e private. La tendenza negli ultimi anni è cambiata ed è facile constatare un'ampia consapevolezza (anche se a volte ancora imprecisa e superficiale) della dimensione trasversale e pervasiva della protezione dei dati.

Di ciò è indice una maggiore capacità di risposta dei titolari del trattamento, che riescono a gestire, con riscontri appropriati agli interpelli preventivi, la gran parte delle istanze. Il fenomeno è evidente soprattutto nelle grandi società di servizi (banche, assicurazioni), ma comincia ad affacciarsi anche nelle amministrazioni pubbliche più consapevoli. In questo quadro, un ruolo positivo è sicuramente giocato dalle figure di responsabili *privacy,* oramai piuttosto diffuse, che, coordinando e indirizzando l'azione degli uffici periferici, assicurano una più puntuale e attenta applicazione della legge. In una qualche misura, dall'esperienza di queste nuove figure professionali viene quasi anticipata la funzione del *privacy officer,* ben conosciuta in altri ordinamenti e recentemente inserita nelle bozze del nuovo regolamento comunitario in materia di protezione dei dati personali (cfr. *infra* par. 21.).

Anche altri fattori hanno contribuito a deflazionare la quantità di ricorsi pervenuti: basti pensare alla diffusione di nuovi strumenti alternativi o comunque propedeutici all'instaurazione di una controversia formale (reclami all'Agcom in materia di servizi telefonici e telematici; ricorso ai mediatori civili autorizzati; azione, ai più diversi livelli, dei difensori civici; ruolo, nel settore di riferimento, dell'arbitro bancario finanziario).

Uno spazio rilevante è poi svolto dai procedimenti instaurati direttamente dinanzi all'autorità giudiziaria ordinaria secondo la procedura, recentemente emendata, dell'art. 152 del Codice, che riconduce un'ampia serie di procedimenti nell'alveo della giurisdizione

ordinaria e potrà anche far emergere una giurisprudenza variegata in ragione della pluralità dei fori aditi.

Non va poi dimenticata la funzione positiva svolta in questi ultimi anni dai codici deontologici promossi e approvati con il determinante contributo dell'Autorità. Soprattutto il codice relativo ai trattamenti svolti presso i sistemi di informazioni creditizie ha contribuito a dare una cornice normativa di riferimento ad un settore (quello delle cd. "centrali rischi private") che non aveva mai avuto una disciplina (se non di tipo contrattuale) e che aveva alimentato, fra il 2002 e il 2005, un contenzioso "alluvionale".

Va anche considerato il largo utilizzo degli altri strumenti di tutela previsti dal Codice, il reclamo e la segnalazione, rispetto ai quali, negli ultimi anni l'Ufficio, anche sulla scorta del regolamento sulle procedure aventi rilevanza esterna, ha sicuramente affinato e velocizzato la propria capacità di risposta.

Oltre a queste ragioni, in qualche misura sistemiche, vanno però evidenziate le ricadute determinate dall'applicazione delle disposizioni contenute nel cd. "decreto Monti" della fine del 2011. Più specificamente e come più volte segnalato nella presente Relazione, l'art. 40, comma 2, del d.l. 6 dicembre 2011, n. 201 (convertito dalla l. 22 dicembre 2011, n. 214) modificando la definizione di "dato personale" e di "interessato", ha largamente sottratto le persone giuridiche, gli enti e le associazioni all'ambito di applicazione della disciplina in materia di protezione dei dati personali. È così venuta meno la possibilità per tali soggetti di avvalersi degli strumenti di tutela previsti dall'art. 7 del Codice, e conseguentemente di attivare il procedimento di ricorso.

Nel flusso di ricorsi del 2012 l'effetto della nuova normativa è stato subito percepibile. Da una parte molti soggetti hanno dovuto forzatamente rinunciare alla possibilità di presentare ricorso, dall'altra è evidente, non solo nei primi mesi dell'anno, l'aumento di declaratorie di inammissibilità che si sono rese necessarie in rapporto a procedimenti iniziati prima dell'entrata in vigore della disposizione o proposti nelle settimane immediatamente successive, quando la percezione dell'impatto delle nuove disposizioni non era ancora chiaro, nonostante le riserve e le preoccupazioni subito espresse al riguardo dal Garante (provv. 19 dicembre 2012 [doc. web n. 2286411]).

L'aspetto paradossale della modifica normativa in parola è che la stessa ha ridotto (se non azzerato) la possibilità, soprattutto per le società commerciali, di proporre istanze di accesso ai dati personali e, in particolare, di avanzare richieste di cancellazione o di opposizione al trattamento dei dati (profili utili tra l'altro nei confronti dell'attività svolta dalle centrali rischi, dalle società di informazione commerciale), privando così molti operatori economici della possibilità di controllare il corretto uso di informazioni che possono, qualora inesatte o incomplete, incidere pesantemente sull'immagine e conseguentemente sulla reputazione economica di un soggetto.

Fornite queste chiavi interpretative di carattere generale, la lettura dei dati statistici è comunque sempre utile. Quanto alla tipologia delle decisioni adottate, va rimarcata l'assoluta prevalenza delle declaratorie di non luogo a provvedere (ben 140 su 233 provvedimenti adottati). È questo un termometro di buon funzionamento del procedimento di ricorso che riesce ad assicurare una rapida ed efficace soddisfazione alle richieste dell'interessato. Molto spesso infatti il mero intervento dell'Autorità in sede istruttoria induce il titolare del trattamento a comunicare i dati personali richiesti o comunque a riscontrare le altre richieste dei ricorrenti, "rimediando" in sede contenziosa al silenzio o ai dinieghi che avevano seguito la ricezione degli interpelli preventivi.

Non va poi trascurato un altro elemento che, per esigenze di semplificazione, non emerge dalle tabelle statistiche: la presenza nei provvedimenti decisori, di più statuizioni in ragione della pluralità di richieste formulate. Non è infrequente l'adozione di provvedimenti che contengono uno spettro completo che va dall'accoglimento di alcune richieste, all'infondatezza e inammissibilità di altre. Al riguardo si segnala, in particolare, la diffusa tendenza ad inserire richieste non riconducibili all'esercizio degli specifici diritti in materia di protezione dei dati personali, quali quelle di risarcimento del danno o volte a evidenziare l'asserita illegittimità di determinati rapporti contrattuali. Ciò soprattutto in quell'ambito bancario e finanziario che, dal punto di vista delle categorie di titolari del trattamento, rappresenta da anni il settore nel quale si concentra il maggior numero di procedimenti.

18.3. PROFILI PROCEDURALI

Dall'ampia giurisprudenza del Garante continuano ad emergere, anche in ambito strettamente procedurale, profili che permettono di approfondire l'esame delle disposizioni di cui agli artt. 145 e ss. del Codice.

Va anzitutto ricordato che lo "spazio" di tutela apprestato dal ricorso, per quanto ampio in ragione della latitudine dei diritti di cui all'art. 7 del Codice che ne costituiscono il presupposto, non è però espandibile fino a comprendere qualunque asserita violazione della riservatezza. In questo senso vengono ancora con una certa frequenza sottoposte al Garante vicende nelle quali si controverte su un utilizzo di dati da parte di persone fisiche, per finalità esclusivamente personali, ad esempio al fine di apprestare la propria difesa in giudizio (provv. 15 marzo 2012 [doc. web n. 1889091]), senza tener conto che tali questioni esulano dall'ambito di applicazione del Codice ai sensi dell'art. 5, comma 3. Oppure si richiede al titolare del trattamento non solo di conoscere le informazioni personali dallo stesso detenute, ma anche di rielaborare i dati stessi secondo modalità di interesse del ricorrente, o anche di aggregarli in modo non corrispondente alle modalità con le quali gli stessi, allo stato, sono conservati (provv. 11 ottobre 2012 [doc. web n. 2131862]): quasi che, con l'intervento del Garante, una informazione (magari una serie di dati contabili) possa essere "trasformata", ad esempio, in un documento contenente la rielaborazione di calcoli "costruiti" in modo da diventare un elemento di prova da produrre in una vertenza di lavoro o in una controversia previdenziale.

Così come, ancora troppo spesso, le pur ampie prospettive aperte dal diritto di accesso ai dati vorrebbero essere piegate, in relazione normalmente ad esigenze di carattere processuale, verso una esclusiva richiesta di acquisizione di copia di documenti, confondendo e sovrapponendo altri strumenti di tutela (l. n. 241/1990 in materia di accesso alla documentazione amministrativa, o le possibilità offerte dal cd. "Testo unico bancario" (T.u.b.) e, in particolare, dal suo art. 119).

Merita poi di essere ricordato il vincolo che impone di esperire la procedura dell'interpello preventivo prima di proporre formalmente il ricorso. In realtà, se questo principio è abbastanza noto, è però ancora diffusa la tendenza ad un suo "aggiramento" attraverso la presentazione di ricorsi proposti in via diretta per asseriti motivi d'urgenza, che però non

reggono all'esame della documentazione inoltrata. Ciò per la palese inesistenza del pregiudizio "imminente e irreparabile" che solo potrebbe giustificare il mancato inoltro dell'interpello preventivo, tenuto anche conto che il lasso di tempo che deve intercorrere prima di rivolgersi al Garante è comunque limitato a quindici giorni. Troppo spesso capita così di constatare come si confonda la necessità di provare l'effettiva impossibilità di attendere anche pochi giorni con situazioni nelle quali si lamenta invece la persistenza di un danno che si sarebbe però già prodotto, a volte anche da mesi (provv. 29 novembre 2012 [doc. web n. 2248935]).

Inoltre, soprattutto con riferimento all'ambito societario, bancario e assicurativo, occorre spesso richiamare l'attenzione degli interessati sulla necessità che l'atto di ricorso sia proposto nei confronti del solo titolare del trattamento, il quale, qualora siano stati formalmente individuati dei responsabili *ex* art. 29 del Codice, dovrà eventualmente dar conto anche del trattamento da essi svolto (provv. 15 novembre 2012 [doc. web n. 2286264]).

Va infine segnalata la particolare ipotesi dell'art. 9, comma 3, che disciplina il diritto di accesso ai dati personali riferiti a persone defunte. È un diritto ad ampio spettro riconosciuto "*a chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione*". È una posizione frequentemente attivata e funzionale, in modo particolare, all'acquisizione di informazioni atte a ricostruire compiutamente l'asse ereditario o a "recuperare" quei dati di carattere clinico che possono eventualmente sostanziare un'istanza risarcitoria per responsabilità medica (provv. 21 marzo 2012 [doc. web n. 1889154]).

18.4. PROCEDIMENTO DI RICORSO E ORGANI COSTITUZIONALI

Pur attenendo formalmente a profili procedurali, merita separata considerazione la problematica connessa alla presentazione di ricorsi nei confronti di organi costituzionali dello Stato (in particolare organi parlamentari). Il tema non è inedito visto che un caso significativo aveva già portato ad un pronunciamento nel 2009 (provv. 16 luglio 2009 [doc. web n. 1638472]), ma è tornato d'attualità nell'anno trascorso con un ricorso deciso il 19 luglio 2012 [doc. web n. 2065905]. Entrambe le vicende si sono chiuse con una declaratoria di inammissibilità, ma la novità e complessità della questione, e soprattutto il significato e la

delicatezza dei valori costituzionali sottesi hanno indotto il Garante a proseguire la riflessione sulla ricerca di un possibile equilibrio fra le contrastanti posizioni in rilievo.

Come noto, il problema nasce dall'ampia e agevole disponibilità in rete della documentazione integrale dell'attività delle Camere nel corso delle legislature repubblicane. La varietà e quantità dei documenti resi facilmente accessibili grazie all'indicizzazione operata dai motori di ricerca generalisti ha naturalmente immesso in rete e, in qualche modo "riattualizzato", una messe di dati personali spesso delicati, anche quando non formalmente ascrivibili al campo dei cd. "dati sensibili". Pertanto molte persone, occasionalmente citate in documenti tipici dell'azione parlamentare (quali interrogazioni, relazioni di commissioni d'inchiesta) hanno fatto leva sul Codice per opporsi a questo trattamento, quanto meno per sollecitare l'interdizione delle pagine e delle notizie dall'azione dei motori di ricerca esterni ai siti di Camera e Senato o per chiedere l'integrazione o la correzione di notizie inesatte o incomplete. Com'è noto rispetto alla vicenda del 2009 gli organi parlamentari hanno richiamato la piena autonomia e insindacabilità nell'esercizio delle funzioni e delle prerogative parlamentari ed il principio costituzionale della pubblicità degli atti parlamentari, mentre per il caso dello scorso anno, pur ribadendo i richiamati princìpi, hanno invocato il disposto dell'art. 8, comma 2, lettera *c),* del Codice, che preclude l'utilizzo dello strumento del ricorso (e dei sottostanti diritti dell'art. 7) nei confronti dei trattamenti svolti dalle Commissioni parlamentari d'inchiesta (nel caso di specie la Commissione antimafia).

Il Garante ha condiviso, sul piano formale-procedurale, queste impostazioni (che hanno portato, come detto, a due pronunce di inammissibilità) ma, sul versante sostanziale, non ha cessato di ricercare un possibile equilibrio più avanzato, anche tenendo conto di una parallela, per quanto limitata, giurisprudenza di merito, che si è mossa in questo medesimo campo senza timidezza (v. Trib. Civ. di Roma, 1ª sez., sentenza 19 gennaio 2012). Ha fatto seguito uno scambio di note, alla fine di luglio 2012, fra il Presidente della Camera dei deputati e il Presidente dell'Autorità, al fine di promuovere ulteriori approfondimenti tecnici e giuridici tra gli uffici interessati, finalizzati, almeno nella prospettiva dell'Autorità, ad individuare misure (quali la deindicizzazione dei testi) idonee ad evitare che, attraverso la pubblicazione *online* di atti parlamentari, si possano ledere diritti e libertà fondamentali.

18.5. LA CASISTICA PIÙ SIGNIFICATIVA

Secondo uno schema ormai collaudato, dopo l'esame dei profili generali si propone una succinta rassegna dei settori più significativi in relazione ai quali sono stati presentati ricorsi, al fine di mettere in luce sia le linee applicative e interpretative ormai consolidate, sia i profili di novità emersi nel corso dell'anno.

Trattamenti svolti presso sistemi di informazioni creditizie e società di informazione commerciale

Il settore delle informazioni creditizie e commerciali è fra quelli più frequentemente oggetto di ricorso, fin dalla prima vigenza della l. n. 675/1996, sul quale il Garante ha finito per assumere al tempo stesso il ruolo di "regolatore" del sistema e di "tutore" delle posizioni individuali incise, anche per l'assenza di specifica normativa, in qualche misura colmata dall'adozione del codice deontologico in materia di sistemi di informazioni creditizie (in vigore dal 1° gennaio 2005), che rappresenta il punto di riferimento anche per l'esame dei ricorsi in materia.

L'esperienza maturata nel 2012 ha confermato l'utilità e il valore deflazionante (in termini di procedimenti attivati) delle disposizioni deontologiche, ma ha anche evidenziato (con riferimento per esempio, alla tempistica di conservazione dei cd. "dati negativi" o alle modalità di inoltro del preavviso di inserimento in banca dati) l'utilità di una revisione delle medesime norme a suo tempo concordate, tenendo conto della diffusione delle tecnologie digitali.

L'eventuale avvio dei lavori di revisione potrebbe essere poi occasione propizia per "rileggere" il codice alla luce di alcuni fatti nuovi recentemente intervenuti, che consigliano uno sguardo aperto alle prospettive future (basti pensare alle modalità di attuazione della recente disposizione che permetterebbe ai fornitori di servizi di comunicazione elettronica di avere accesso ai Sic -Sistemi di informazioni creditizie-, al dibattito sull'opportunità di creare nuove "centrali rischi" in diversi ambiti merceologici o di estendere l'ampiezza delle informazioni contenute negli attuali Sic, fino alle prospettive ed ai problemi che possono interessare il settore alla luce del nuovo assetto normativo comunitario in corso di elaborazione).

Se rispetto ai trattamenti svolti presso i Sic il codice deontologico del 16 novembre 2004 fornisce una piattaforma di regolazione efficace e condivisa, tutt'altra situazione caratterizza i trattamenti riguardanti il settore dell'informazione commerciale, che parimenti dà luogo ad un importante contenzioso dinanzi all'Autorità. È anche questo un ambito che interessa un

elevatissimo numero di soggetti (tutto il sistema imprenditoriale che viene censito per offrire informazioni sulla solidità e affidabilità delle imprese a chi a vario titolo deve operare con le stesse) dove la precisione e la completezza delle informazioni hanno un valore essenziale, poiché un dato errato può compromettere, a volte, la stessa sopravvivenza sul mercato di un operatore. È innegabile, però, la complessità della materia e la conseguente difficoltà di una *reductio ad unitatem* della stessa.

Se infatti i Sic sono caratterizzati da una sostanziale omogeneità di dati (rapporti finanziari riconducibili al cd. "credito al consumo" concessi alla platea dei consumatori-persone fisiche), il settore delle informazioni commerciali, da una parte, fa riferimento ad un *target* più limitato (le imprese commerciali) dall'altra, però, associa a tale platea una quantità di informazioni eterogenee (ad es., fatte dal registro delle imprese, dagli archivi dei tribunali concernenti le procedure fallimentari, dal catasto, dal registro dei protesti) che scontano una disciplina di riferimento diversa, nonché modalità di trattamento e tempi di conservazione differenziati, anche in ragione delle funzioni diverse cui i vari archivi sono funzionalmente preposti. Ne deriva l'esigenza di fare chiarezza, apprestando una serie di regole condivise che contemperino la necessità di informazioni sempre più estese e complete che viene dal sistema economico e finanziario e l'obbligo di assicurare che i dati siano esatti, completi, aggiornati, qualitativamente significativi.

In questo quadro si collocano le iniziative del Garante per giungere alla redazione di un codice deontologico di settore, che hanno incontrato il favore degli operatori, ma che sicuramente scontano la difficoltà di un quadro normativo instabile. È di tutta evidenza che le già segnalate modifiche alle nozioni base di "dato personale" e di "interessato", incidendo sulla collocazione, nel sistema *privacy,* delle società commerciali, hanno di fatto precluso la possibilità di estendere la disciplina deontologica a quel complesso di *report* e *dossier* esplicitamente riferiti a società ed enti pubblici e privati di ogni tipo. Ma suscitano perplessità i recenti tentativi, in sede parlamentare, di sottrarre all'ambito di applicazione del Codice anche i trattamenti di dati concernenti le persone fisiche preposte ai ruoli di vertice nelle gerarchie societarie.

Trattamenti in ambito assicurativo

Nel settore assicurativo l'esame del contenzioso fa emergere il delicato ruolo di equilibrio del Garante di contemperamento fra contrastanti interessi: nel caso di specie, da un lato, il

diritto di accesso rivendicato dagli interessati cui i dati si riferiscono, dall'altro le esigenze di tutela delle compagnie di assicurazione.

È tipica infatti della dinamica dei rapporti assicurativi la contrapposizione fra i soggetti che hanno subìto danni, o che comunque chiedono risarcimenti, e le compagnie chiamate all'eventuale liquidazione di tali richieste.

Nell'intreccio di questi rapporti, inevitabilmente conflittuali, si inseriscono acquisizione di informazioni e testimonianze, raccolta di dati medici, svolgimento di perizie medico-legali, tutte operazioni che comportano un esteso utilizzo di dati sensibili e, a volte, giudiziari.

È evidente che, nel momento in cui le reciproche posizioni o pretese non trovano una composizione bonaria e sfociano in una vertenza giudiziaria o anche solo in una dialettica pre-contenziosa, la tempestiva disponibilità di determinati dati personali può assumere un rilievo determinante per l'esito di una vertenza. Perciò tutela (o meglio possibilità di disporre) dei dati di un interessato e necessità di non compromettere le esigenze difensive e processuali del titolare del trattamento (che ha interesse non a nascondere o distruggere certe informazioni, ma sicuramente a differirne l'ostensione in un momento processualmente propizio) si confrontano e si scontrano, anche davanti all'Autorità.

È un contrasto inevitabile, in qualche modo preventivato dallo stesso legislatore che, nell'art. 8 del Codice, ha ipotizzato la possibilità di invocare, da parte del titolare del trattamento, il differimento dell'accesso ai dati proprio nell'ipotesi in cui il "disvelamento" delle informazioni determini "*un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria*". Da ciò la necessità di effettuare un'attenta valutazione in concreto, per verificare l'esistenza di questi elementi "escludenti" il normale esercizio del diritto di accesso (provv. 8 marzo 2012 [doc. web n. 1889056]). Senza dimenticare che l'art. 8, comma 4, più radicalmente esclude dall'ambito di applicazione della disciplina l'indicazione di decisioni in via di assunzione da parte del titolare del trattamento o considerazioni a carattere difensivo o di strategia contrattuale o processuale, magari espresse in pareri resi dai legali di fiducia o da qualche consulente incaricato (provv. 29 novembre 2012 [doc. web n. 2286291]).

Come già detto, il settore bancario ha visto la presentazione del più elevato numero di ricorsi, specie in relazione all'esercizio del diritto di accesso. In qualche modo, l'utilizzo di tale diritto ha prima affiancato e poi quasi surclassato gli strumenti di tutela previsti dal Testo unico bancario (T.u.b.). Tale fenomeno ha determinato qualche incomprensione e qualche confusa sovrapposizione fra le diverse previsioni, in relazione alle quali il Garante è dovuto più volte intervenire per chiarire i diversi ambiti di applicazione. In particolare, dinanzi all'Autorità può essere fatto valere solo il diritto di accesso ai dati personali riferiti all'interessato/ricorrente, che non deve essere confuso con l'accesso a documenti bancari disciplinato dall'art. 119 del citato T.u.b. (provv. 20 settembre 2012 [doc. web n. 2106524]). In questo quadro va ricordata l'inammissibilità di richieste di accesso volte soprattutto a conoscere dati di terzi (ad es., beneficiari di determinate operazioni bancarie), oppure ad acquisire la copia di documenti che in realtà non contengono neppure dati personali (ad es., prospetti informativi relativi alla quotazione in borsa di una società), oppure richieste finalizzate ad ottenere un'aggregazione di dati, anche personali, non nelle forme in cui gli stessi risultano conservati negli archivi del titolare, ma secondo criteri e modalità suggeriti dalle particolari esigenze del richiedente.

Merita poi di essere considerato il profilo relativo all'onere connesso al riscontro delle predette richieste di accesso. Al riguardo si deve ricordare che tali richieste devono essere riscontrate gratuitamente, senza addossare all'interessato oneri previsti per altri tipi di operazioni e servizi bancari (provv. 26 luglio 2012 [doc. web n. 2104639]). Il tema viene spesso riproposto visto che, in effetti, questo tipo di richieste si sta diffondendo e a volte la loro estensione temporale e la loro complessità determina, da parte degli istituti di credito, l'impiego di mezzi e risorse non indifferenti.

Va infine posta attenzione ai tempi di conservazione dei dati. Le richieste formulate nei confronti degli istituti di credito sono infatti caratterizzate da un'ampia profondità temporale, nel tentativo, sotteso a molte istanze, di ricostruire integralmente i rapporti con una banca fin dall'instaurazione del rapporto. Va però ricordato che non è prevista una conservazione per un tempo indefinito dei dati e delle informazioni bancarie (situazione che si porrebbe in evidente contrasto con il principio generale di conservazione limitata nel

tempo di cui all'art. 11, comma 1, lett. *e),* del Codice). Anzi esiste, sulla base di specifici obblighi normativi, la previsione di un termine decennale di conservazione che rappresenta, quindi, il limite massimo di tempo rispetto al quale formulare un'istanza di accesso.

Trattamento dei dati in ambito giornalistico

Come già segnalato (cfr. *supra* par. 18.1.) ormai l'attenzione e la sensibilità degli interessati si rivolgono sempre più spesso nei confronti dei periodici *online* o comunque delle nuove forme di manifestazione del pensiero disponibili sulla rete (*blog*, *forum* di discussione, siti internet della più varia natura ed altro). È un terreno nuovo, in larga misura inesplorato, sul quale ancora una volta il Garante è chiamato a fare da apripista, in qualche misura anche in vista della eventuale definizione di adeguati parametri legislativi (problema che peraltro non riguarda solo l'Italia, poiché le incertezze al riguardo dominano il dibattito a livello mondiale). In questo quadro già complesso ha determinato un effetto moltiplicativo delle problematiche la rapida diffusione degli archivi *online,* che permettono di disporre permanentemente e di accedere con semplicità (tramite i motori di ricerca generalisti) alle raccolte complete dei quotidiani e dei periodici di informazione, con una profondità temporale addirittura di decenni, che permette quindi di riportare ad attualità anche il più lontano passato. È evidente infatti che, in questa situazione, alcuni valori, tutti costituzionalmente rilevanti, entrano in forte tensione e tendono a confliggere. Dalla libertà di manifestazione del pensiero e in particolare dall'esercizio del diritto di cronaca e di critica che aveva ispirato *ab origine* determinate pubblicazioni (gli articoli originari, spesso risalenti nel tempo, che, in ipotesi, contengono informazioni delicate, negative, sgradite…) al diritto di libera ricerca, in particolare storica, fondato sulla possibilità di disporre di archivi quanto più estesi e completi (che ovviamente si avvantaggia di tecnologie che permettono comodamente e gratuitamente l'accesso ad archivi di tali dimensioni) fino al contrapposto interesse di tanti soggetti citati nella miriade di articoli messi in rete che ben possono ricevere nocumento da questa sorta di "ripubblicazione virtuale permanente" e che aspirano quindi a veder riconosciuto quel "diritto all'oblio" che nell'era di internet presenta profili particolarmente problematici.

Fin dal 2009 (come segnalato anche nelle precedenti Relazioni annuali) il Garante ha individuato una possibile soluzione nella cd. "deindicizzazione", dai motori di ricerca generalisti, di quelle informazioni che, volta a volta, sulla base di un'accurata analisi del caso

specifico, potevano incidere in modo effettivamente sproporzionato sui diritti degli interessati citati nelle cronache giornalistiche. Tutto ciò tenendo conto di alcuni criteri di ragionevolezza e buon senso ricavati dall'ampia casistica che si è presentata in questi anni (attenzione alle richieste delle persone non note, delle vittime di reato, dei terzi incidentalmente citati; valutazione del tempo trascorso dalla vicenda narrata e della posizione di notorietà o meno, nell'ambito geografico di riferimento della testata giornalistica, della persona citata e soprattutto accertamento sulla attuale persistenza di elementi che giustifichino tuttora un'ampia divulgazione di notizie pur datate). Il panorama è complesso e difficilmente sussumibile in schemi di carattere generale, sicché il Garante ha preferito procedere caso per caso senza elaborare, fino a questo momento, linee di condotta predeterminate e astratte.

Anche il 2012 ha portato significative decisioni in merito (provv.ti 4 ottobre 2012 [doc. web n. 2108032] e 18 ottobre 2012 [doc. web n. 2130029]), ma soprattutto ha indotto l'Autorità a deliberare su un profilo diverso e per certi aspetti ulteriore rispetto a quello fin qui analizzato. Sono infatti pervenuti diversi ricorsi nei quali la richiesta volta ad ottenere che un determinato articolo non venisse più indicizzato dai motori di ricerca esterni al cd. "sito sorgente" (normalmente quello dell'editore di una testata giornalistica dotato di un archivio storico *online*) veniva accompagnata o da una richiesta di cancellazione integrale dell'informazione dal sito web dello stesso giornale, o da una parallela richiesta di integrazione e aggiornamento dell'informazione a suo tempo fornita.

Sono evidenti le implicazioni delicate e significative di questo nuovo "fronte". Per quanto concerne il primo aspetto, non può sfuggire l'effetto che una cancellazione "totale" di una notizia può apportare sull'integrità di una fonte, sulla completezza e sulla ricostruibilità di una pubblicazione storicamente avvenuta, specie quando la stessa dovesse essere disponibile esclusivamente in formato digitale. È chiaro quindi che interventi di "rimozione" devono trovare una base giuridica e una giustificazione fondata. Sono parametri che, ad esempio, non si riscontrano quando le informazioni riportate sono veritiere, i fatti sono recenti e la vicenda narrata (magari di tipo processuale) è ancora in corso e suscettibile di ulteriori sviluppi e aggiornamenti (provv. 8 marzo 2012 [doc. web n. 1887094]).

Non meno delicato è il secondo problema (quello dell'aggiornamento di una notizia) che inevitabilmente comporta riflessi su normative e competenze che eccedono il terreno esclusivo della protezione dei dati personali. Sicuramente le ipotesi sulle quali si è focalizzata l'attenzione non sono quelle nelle quali si voglia discutere di una "rettifica" di una notizia pubblicata, profilo per il quale la legge sulla stampa ha apprestato strumenti utilizzabili (almeno in riferimento alle testate giornalistiche registrate) né quelle nelle quali si faccia questione di lesioni all'onore e alla reputazione di un soggetto, profili questi che rimandano al giudice penale o all'attivazione di azioni risarcitorie in sede civile.

Gli aspetti che hanno coinvolto direttamente il Garante riguardano piuttosto l'esercizio di quei diritti (integrazione e aggiornamento dei dati) che rientrano pienamente nel campo di applicazione della legge sulla protezione dei dati personali. Si tratta di situazioni nelle quali la deindicizzazione degli articoli in questione dai motori di ricerca generalisti era già stata effettuata, ma il ricorrente aveva messo in luce la necessità di aggiornare le cronache comunque disponibili in modo integrale nel cd. "sito sorgente", alla luce dei rilevanti sviluppi che la vicenda in origine raccontata aveva avuto, ma che non erano stati oggetto di successiva cronaca giornalistica.

La situazione è abbastanza tipica di quei casi di cronaca giudiziaria che, per le più varie ragioni, godono, nella fase iniziale, da parte dei *mass media,* di una grande attenzione, che però generalmente tende a sfumare con l'andare del tempo e non segue pertanto molte vicende fino alla loro conclusione. Le conseguenze sulla vita e sull'identità personale degli interessati, nonché sul loro profilo professionale sono chiaramente pesanti, specie quando si tratta di professionisti affermati o di persone attive nel campo economico-finanziario, ambiti nei quali la reputazione personale è un valore non negoziabile.

È significativo che il tema sia stato oggetto nello stesso periodo di un importante pronunciamento della Corte di Cassazione che con la sentenza n. 5525/2012 ha affrontato la medesima problematica, sottolineando la necessità di dar conto di successive evoluzioni di una vicenda già oggetto di cronaca giornalistica. Ciò perché non si può prescindere dall'informazione su tali sviluppi "*giacché altrimenti la notizia, originariamente completa e vera, diviene non aggiornata risultando quindi parziale e non esatta, e pertanto sostanzialmente non*

vera". Anche ispirandosi a questo importante pronunciamento, il Garante in due occasioni ha accolto ricorsi aventi ad oggetto la richiesta di aggiornare, sulla base di significativi sviluppi avvenuti *medio tempore*, gli articoli (già deindicizzati) presenti sul sito di un'importante testata giornalistica. In particolare si è ordinato all'editore resistente di predisporre un idoneo sistema nell'ambito dell'archivio storico *online* in cui gli articoli sono conservati per segnalare, appunto (ad es., con un'annotazione a margine dei singoli articoli) l'esistenza del "seguito", o dello "sviluppo" della notizia, in modo da assicurare, da un lato, all'interessato il rispetto della propria (attuale) identità personale, quale risultato della completa visione di una serie di fatti che lo hanno visto protagonista (anche se solo in parte oggetto di cronaca giornalistica), dall'altro, ad ogni lettore, un'informazione attendibile e completa (provv.ti 20 dicembre 2012 [doc. web n. 2286432] e 24 gennaio 2013 [doc. web n. 2286820]).

È evidente che decisioni di questa portata devono essere sottoposte ad un vaglio critico attento, specie tenendo conto delle difficoltà della loro esecuzione (basti pensare ad ipotizzabili dispute sui contenuti concreti delle integrazioni da effettuare, o alle ipotesi in cui non sia chiaramente desumibile, da atti e documenti, l'esistenza stessa di un reale aggiornamento di cui dar conto). Al riguardo potrebbe essere utile esaminare la tematica in un confronto aperto, in particolare, a giornalisti ed editori, per "gestire" quello che, prima di essere un problema di contenzioso, è in realtà una nuova frontiera dell'informazione.

19. Il contenzioso giurisdizionale

19.1. Considerazioni generali

Come riferito nella Relazione 2011 (p. 161), l'art. 34 del d.lgs. n. 150/2011 ha abrogato l'art. 152 del Codice -con l'eccezione del comma 1- dettando all'art. 10 nuove regole procedurali concernenti le controversie sull'applicazione del Codice.

È stato altresì abrogato il comma 7 dell'art. 152, che prevedeva esplicitamente l'obbligo della notifica al Garante dei ricorsi proposti direttamente davanti all'autorità giudiziaria, non coinvolgenti le pronunce dell'Autorità.

Tale abrogazione ha fatto sentire i suoi effetti negativi sul numero delle notifiche relative a tale tipologia di giudizi effettuate al Garante, che in alcuni casi l'autorità giudiziaria ha continuato a ritenere necessarie; a fronte dei 170 nel 2011, nel 2012 sono stati notificati all'Autorità e da questa trattati 78 ricorsi.

Attesa la accertata utilità della tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, attestata dal costante aumento del numero delle notifiche all'Autorità effettuate negli anni precedenti, assume sempre maggiore rilevanza l'obbligo -purtroppo non sempre puntualmente adempiuto- per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

Tale trasmissione, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà necessarie, potrà consentire al Garante di continuare ad avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo gli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f)*, del Codice).

19.2. I profili procedurali

L'art. 152 devolve tutte le controversie riguardanti l'applicazione del Codice all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento (art. 10, comma 2, d.lgs. n. 150/2011).

In particolare, il comma 3 dell'art. 10 del d.lgs. n. 150/2011, riportando pedissequamente il testo dell'abrogato art. 152, comma 3, del Codice, ricomprende in dette controversie quelle proposte avverso i provvedimenti del Garante.

Nonostante tale chiara attribuzione di competenza, è stata proposta un'opposizione davanti al Giudice di pace di Milano avverso un atto istruttorio adottato dal Garante nell'ambito di un procedimento su ricorso proposto ai sensi dell'art. 145 del Codice, con il quale l'istante aveva avanzato richiesta di accesso ai dati relativi al nominativo del soggetto che aveva richiesto l'emissione di un assegno circolare. In giudizio, l'Autorità aveva eccepito l'incompetenza sia funzionale sia territoriale del giudicante, essendo competente il Tribunale di Torino, ove ha sede l'istituto di credito titolare del trattamento. Con la sentenza n. 100.029 del 7 gennaio 2013, con cui ha respinto l'opposizione, il Giudice di pace ha invece ritenuto sussistente la propria competenza, sul rilievo che l'attore non era cliente della banca, ma solo giratario dell'assegno.

In tema di giurisdizione, analogamente a quanto accaduto nel 2011, nel 2012 l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

Non si sono altresì riscontrate pronunce che hanno dichiarato un difetto di competenza per materia.

È giunto invece a conclusione il procedimento introdotto dal ricorso straordinario al Presidente della Repubblica nei confronti del provvedimento del 22 dicembre 2009 [doc. web n. 1695144], con il quale l'Autorità aveva respinto il ricorso con cui l'interessato aveva chiesto la cancellazione di dati sensibili riportati in una nota contenuta nel suo fascicolo personale detenuto dal Ministero dell'interno. Confermando l'orientamento precedentemente espresso (sez. prima, n. 4468/2007, v. Relazione 2008 p. 210; sez. prima, n. 3754/2009, v. Relazione 2009 p. 230), il Consiglio di Stato ha ritenuto il ricorso inammissibile (sez. prima, n. 170/2011; v. d.P.R. del 29 ottobre 2012), in quanto avverso atti dell'amministrazione oggetto di tutela giurisdizionale, quale quella prevista dall'art. 152 del Codice, qualificabile come esclusiva e funzionale.

19.3. I PROFILI DI MERITO

Nel 2012 l'autorità giudiziaria ha emesso alcune pronunce, nell'ambito di giudizi nei quali non erano in discussione provvedimenti adottati dal Garante, con riferimento alla divulgazione di dati personali di natura sensibile da parte di una pubblica amministrazione ed al loro trattamento da parte di alcuni istituti di credito.

I ricorrenti, beneficiari di prestazioni indennitarie, contestavano, in particolare, il riferimento da parte dell'ente pubblico erogatore, nella causale di accredito dei fondi ricevuti, al titolo giustificativo costituto dalla l. n. 210/1992 (relativa all'indennizzo a favore dei soggetti danneggiati da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazioni di emoderivati) e la detenzione di tale dato da parte delle banche ove erano stati aperti i conti. Gli istanti chiedevano l'inibitoria della divulgazione di dati personali sensibili e il risarcimento dei danni subiti.

Nel rigettare le domande, il Tribunale di Napoli ha escluso che l'ente pubblico abbia illecitamente propagato i dati sensibili portandoli a conoscenza di soggetti indeterminati, essendosi invece limitato a trasmetterli attraverso una rete informatica ad accessibilità ristretta ad un unico soggetto, ovvero l'istituto di credito che, sulla base del contratto di conto corrente riveste il ruolo, unitamente all'ente pubblico, di titolare del trattamento. Anche nei confronti degli istituti di credito il Tribunale non ha ravvisato alcun illecito, poiché la banca si era limitata, in esecuzione di un preciso obbligo contrattuale, a descrivere la causale del bonifico nei certificati di estratto conto (Trib. di Napoli, sentenza n. 7896 dell'8 luglio 2012; sentenze nn. 5115, 5116 e 5117 del 4 maggio 2012).

Alcune pronunce dell'autorità giudiziaria hanno riguardato, in particolare, le segnalazioni degli interessati come cattivi pagatori, da parte di istituti di credito o società finanziarie ai soggetti che gestiscono i sistemi di informazioni creditizia (Sic) o alla Banca d'Italia, materia che genera frequente contenzioso per il rilievo che assume per gli interessati.

In tre casi la segnalazione è stata riconosciuta non corretta, con condanna dell'istituto o della società che l'aveva effettuata al risarcimento del danno in favore dell'interessato. I casi concernono: un soggetto che era stato segnalato da una società di finanziamento quale garante di un prestito erogato ad altra persona (Trib. di Milano, I sez. civ., sentenza n. 5395

del 10 maggio 2012); una persona segnalata alla Centrale d'allarme interbancaria (Cai), istituita presso la Banca d'Italia, a cui la società emittente aveva revocato la carta di credito (Trib. di Roma, sez. X civile, sentenza n. 23732 del 5 dicembre 2012); un interessato a cui era stato rifiutata la sottoscrizione di un contratto di mutuo fondiario con garanzia ipotecaria, essendovi una segnalazione di sofferenza a suo carico presso la Centrale rischi della Banca d'Italia (Trib. di Milano, I sez. civ., sentenza n. 6265 del 28 maggio 2012).

Nel terzo caso l'ente resistente, oltre al risarcimento del danno, è stato condannato anche alla cancellazione dei dati personali del ricorrente.

In due casi, invece, la segnalazione è stata ritenuta corretta, con conseguente rigetto delle domande di cancellazione e di risarcimento del danno. I casi concernono: ritardi nei pagamenti dovuti all'utilizzo della carta di credito (Trib. di Milano, sentenza n. 6478 del 29 maggio 2012); segnalazione alla Centrale rischi della Banca d'Italia di inadempimenti nei pagamenti relativi ad un contratto di finanziamento (Trib. di Milano, sentenza n. 719 del 28 febbraio 2012).

In un altro caso, pur ritenendo ingiustificata la segnalazione, il giudice ha respinto la domanda di risarcimento del danno, ritenuta non dimostrata (Trib. di Milano, sentenza n. 2887 del 5 luglio 2012).

19.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2012 ha registrato una sostanziale stabilità nella proposizione delle opposizioni a provvedimenti del Garante: a fronte dei settantadue ricorsi del 2011, nel 2012 sono state proposte settantatré opposizioni. Di queste, trentaquattro si riferiscono a opposizioni a ordinanze ingiunzioni, così registrando un calo rispetto al 2011, nel quale si erano registrate quarantacinque opposizioni di tale natura.

Complessivamente l'Autorità ha avuto notizia di trentacinque decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi.

Opposizioni a ordinanze ingiunzioni

Ventidue sentenze hanno avuto ad oggetto opposizioni a ordinanze ingiunzioni; di queste, quindici hanno riguardato violazioni dell'art. 13 del Codice per omessa o inidonea informativa agli interessati, talvolta unitamente all'omessa acquisizione del loro consenso.

Cinque pronunce, riguardanti trattamenti di dati svolti attraverso siti internet da parte di una università telematica, di un esercizio commerciale, di un ente teatrale, di un'azienda di trasporti e, mediante la compilazione di *form*, di un'azienda municipalizzata per la raccolta di rifiuti urbani hanno respinto le opposizioni, confermando i provvedimenti del Garante (Trib. di Roma, sentenza n. 3739 del 4 luglio 2012; Trib. di Busto Arsizio, sentenza n. 143 del 26 aprile 2012; Trib. di Roma, sentenza n. 10729 del 24 maggio 2012).

Nel quarto caso, per l'entità del fatto (in particolare, le finalità non commerciali perseguite con il trattamento dei dati e la circostanza che l'azienda si era prontamente attivata per inserire una corretta informativa sul proprio sito) e nel quinto per le condizioni economiche dell'azienda e l'attività di servizio pubblico espletata, l'accertata violazione è stata considerata di "minore gravità" (art. 164-*bis*, comma 1, del Codice), con conseguente riduzione dell'importo della sanzione (Trib. di Trento, sentenza n. 110 dell'8 febbraio 2012; Trib. di Taranto, sentenza n. 807 del 23 aprile 2012).

Due pronunce, concernenti trattamenti di dati effettuati attraverso la compilazione di *form* sui siti internet di altrettante società per i quali non era stata fornita l'obbligatoria informativa e non era stato acquisito il consenso, hanno respinto l'opposizione, nel primo caso confermando integralmente il provvedimento del Garante e, nel secondo, rideterminando l'ammontare della sanzione pecuniaria (Trib. di Udine, sentenza n. 1332 del 7 novembre 2012; Trib. di Roma, sentenza n. 2969 del 22 febbraio 2012).

In altra pronuncia, anch'essa concernente il rilascio di un'inidonea informativa agli interessati al momento del conferimento di incarico da parte di un intermediario immobiliare, il giudice ha confermato il provvedimento ingiuntivo (Trib. di Perugia, sentenza n. 1221 del 2 ottobre 2012).

Uguale conferma, ma con riduzione della sanzione, è stata decisa dal Tribunale di Reggio Emilia in fattispecie di omessa informativa da parte di un circolo privato (sentenza del 20 febbraio 2012).

Ulteriori due pronunce, aventi ad oggetto il trattamento di dati personali realizzato attraverso l'uso di sistemi automatizzati di chiamata senza l'intervento di operatore e di fax per i quali era stata omessa l'informativa, hanno visto la conferma dei provvedimenti del

Garante (Trib. di Marsala, sentenza n. 175 del 28 febbraio 2012; Trib. di Roma, sentenza n. 8834 del 4 maggio 2012).

Una ulteriore pronuncia, riguardante due ordinanze ingiunzioni emanate nei confronti di una società che aveva inviato fax promozionali senza previamente fornire un'idonea informativa agli interessati e senza avere acquisito il loro consenso, ha confermato entrambi i provvedimenti dell'Autorità (Trib. di Roma, sentenza n. 21089 del 18 aprile 2012).

In un caso, concernente l'omesso adempimento di un provvedimento emanato dall'Autorità (artt. 150, comma 2, e 162, comma 2-*ter*, del Codice), il ricorso è stato proposto avverso il verbale di contestazione di violazione amministrativa.

In sintonia con il consolidato orientamento della Corte di Cassazione, richiamato dal Garante, il ricorso è stato dichiarato inammissibile, in quanto la contestazione non è autonomamente impugnabile, non essendo decisione finale dell'Autorità sulla irrogazione della sanzione, costituita dalla eventuale ordinanza-ingiunzione (Trib. di Roma, sentenza n. 1041 del 18 giugno 2012).

In due opposizioni, riguardanti trattamenti di immagini raccolte attraverso sistemi di videosorveglianza posti all'ingresso di due esercizi commerciali, i giudici aditi, nel confermare i provvedimenti del Garante, hanno però rideterminato l'importo della sanzione pecuniaria (Trib. di Lamezia Terme, sentenza n. 843 del 29 maggio 2012; Trib. di Monza, ordinanza *ex* art. 702-*bis* e ss., c.p.c., del 28 marzo 2012).

Una pronuncia ha avuto ad oggetto la violazione degli artt. 37 e 38 del Codice per omessa o incompleta notificazione del trattamento da parte di una casa di cura. La decisione ha respinto l'opposizione e confermato il provvedimento del Garante (Trib. di Catania, sentenza n. 3241 del 20 febbraio 2012).

La mancata adozione da parte di una società delle misure minime di sicurezza, consistente nella omessa designazione per iscritto degli incaricati del trattamento in violazione dell'art. 30 del Codice e nella mancata adozione di *password* aventi otto caratteri, è stata oggetto della sentenza del Tribunale di Bologna, che ha confermato il provvedimento del Garante. La società aveva lamentato la violazione del principio del *ne bis in idem*, ritenendo che il Garante avesse già irrogato, per lo stesso fatto, un'altra sanzione. Accogliendo le osservazioni del

Garante, il giudice ha invece rilevato che era stata impugnata l'ordinanza-ingiunzione emessa nei confronti della società per la violazione amministrativa prevista dall'art. 162 del Codice, mentre l'importo a cui l'opponente faceva riferimento costituiva atto interno del procedimento penale instaurato, ai sensi dell'art. 169 del Codice, per gli stessi fatti, nei confronti della persona fisica autore della violazione.

Nella specie, quindi, non sussisteva la lamentata violazione del principio del *ne bis in idem* trattandosi di profili e di soggetti diversi (sentenza n. 20333 dell'8 marzo 2012).

Cinque pronunce hanno accolto le opposizioni ad altrettanti provvedimenti ingiuntivi emanati dal Garante.

La prima ha avuto ad oggetto il mancato rispetto, da parte dell'Autorità, del termine di novanta giorni dall'accertamento entro il quale deve avvenire la notificazione della contestazione di violazione amministrativa (Trib. di Bolzano, sentenza n. 199 del 17 febbraio 2012).

La seconda, concernente la raccolta di dati personali tramite un *forum online*, è stata accolta in quanto il provvedimento ingiuntivo era stato adottato nei confronti di uno studio professionale quale autore dell'illecito e non come soggetto tenuto in via solidale al pagamento della somma (Trib. di Latina, sez. di Terracina, sentenza n. 1231 del 26 aprile 2012). Avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Con la terza, riguardante la mancata adozione di una misura minima di sicurezza, consistente nell'omessa designazione, in violazione dell'art. 30 del Codice, di un incaricato del trattamento da parte di una società commerciale, sono state accolte le argomentazioni della società ingiunta, in quanto non è risultata dimostrata la violazione dell'art. 33 del Codice (Trib. di Roma, sentenza n. 10863 del 24 maggio 2012). Anche avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Nella quarta, relativa ad un caso di inidonea informativa riguardo l'utilizzo di una particolare tecnologia per mezzo della quale era possibile identificare gli utenti di un impianto di risalita, il Giudice ha ritenuto esaustiva l'informativa rilasciata dalla società agli utenti in relazione alla raccolta ed all'uso dei dati personali (Trib. di Sondrio, sentenza n. 102 del 12 aprile 2012). Il Garante ha proposto ricorso avanti alla Corte di Cassazione.

Nella quinta, infine, concernente il trattamento svolto da un ente pubblico territoriale tramite il sito internet istituzionale di dati personali idonei a rivelare lo stato di salute dei soggetti inseriti nelle graduatorie provinciali degli iscritti negli elenchi del collocamento obbligatorio dei disabili e dei centralinisti non vedenti, il Tribunale ha ritenuto che, in tema di sanzioni amministrative, autore della violazione è solo la persona fisica che ha commesso il fatto e non la persona giuridica (nei cui confronti era stata emessa l'ordinanza-ingiunzione) che può rispondere solo a titolo di obbligato in solido con l'autore, trattandosi di soggetto nei cui confronti non può essere compiuta alcuna valutazione dell'elemento soggettivo dell'illecito, dell'imputabilità e dell'esistenza di cause di esclusione della responsabilità (Trib. di Avellino, sentenza n. 374 del 29 febbraio 2012). Anche in questo caso il Garante ha proposto ricorso avanti alla Corte di Cassazione.

Ambito territoriale di applicazione del Codice

Particolare interesse presenta, anche per i complessi profili tecnici coinvolti, una sentenza del Tribunale di Milano con riferimento all'art. 5, comma 2, del Codice, ai sensi del quale le norme del Codice stesso non si applicano al trattamento di dati personali effettuato da chi è stabilito nel territorio di un Paese non appartenente all'Unione europea anche se impiega per il trattamento strumenti situati nel territorio dello Stato, ma solo ai fini di transito nel territorio dell'Unione.

A seguito di numerose segnalazioni ricevute relative alla ricezione di fax non richiesti a carattere promozionale, il Garante, a seguito di una complessa attività istruttoria, aveva individuato la società che per conto di terzi aveva trasmesso tali comunicazioni dichiarando illecito il trattamento dei dati (provv. 7 aprile 2011 [doc. web n. 1810207]).

La società aveva impugnato il provvedimento sostenendo che l'intero processo dei messaggi pubblicitari era gestito su *server* collocati negli Stati Uniti e che parte del servizio fax diretto verso l'Italia veniva indirizzato presso un *delivery node* in Italia, gestito da una società telefonica ivi stabilita, sicché a parte il mero transito della comunicazione, nessun trattamento sui messaggi veniva realizzato in Italia, con conseguente applicabilità dell'esimente di cui all'art. 5, comma 2, del Codice.

Il Garante ha rilevato in giudizio che, in base alla normativa italiana (delibera Agcom 417/06/CONS, in G.U. 7 settembre 2006, n. 208; delibera 180/10/CONS, in G.U. 28

maggio 2010, n. 123), il "servizio di transito" consiste nel mero trasporto di traffico da una rete di origine a una di terminazione.

La società, invece, effettuava il trattamento dati attraverso una struttura informatica complessa, che inoltrava al mittente (cioè al terzo nel cui interesse erano svolte le attività promozionali), per ogni destinatario, un messaggio contenente l'esito della spedizione del singolo fax, tracciando le informazioni relative all'invio, in particolare l'utenza e l'indirizzo *Ip* del mittente, il numero del fax del destinatario, l'esito dell'invio, il numero dei fax inviati e il contenuto del messaggio. Il sistema realizzava, pertanto, una interconnessione tra la rete internet e la rete telefonica, attuabile, secondo le attuali conoscenze tecniche, attraverso uno specifico dispositivo di interconnessione, noto come fax *gateway* che, per la realizzazione del servizio offerto dalla società resistente, deve necessariamente trattare alcuni dati personali, tra i quali la conversione di un identificativo di utente della rete internet in un numero di abbonato della rete telefonica pubblica; la ricezione del fax al fine di acquisirne l'immagine; la conversione del formato dell'immagine. Il Garante ha, altresì, accertato che il fax *gateway* si trovava nel territorio italiano ed era gestito direttamente dalla società.

Tutto ciò ha consentito di provare che la società ispezionata era titolare di un trattamento di dati personali effettuato in Italia, ancorché con dati detenuti all'estero (cioè nei *server* dove i clienti della ricorrente caricano le informazioni) che, pertanto, ricadeva sotto l'applicazione del Codice.

Il Tribunale di Milano, con sentenza n. 3352 del 2 aprile 2012, ha accolto interamente le tesi sostenute dal Garante.

Informativa nell'intermediazione per la ricerca del personale

Si ritiene utile dare diffusamente conto anche di un'interessante decisione del Tribunale di Udine, sezione distaccata di Cividale del Friuli che, per quanto depositata nel 2010, è pervenuta al Garante nel luglio 2012.

In particolare, il Tribunale ha affrontato il tema dell'obbligo di informativa posto dall'art. 13 del Codice in un caso nel quale il titolare di un'azienda individuale si era rivolto ad una società di intermediazione per il reperimento di rappresentanti di commercio attraverso il sito internet dell'intermediario. L'azienda, che era stata sanzionata per non avere reso l'informativa agli agenti che producevano il loro *curriculum*, aveva impugnato il provvedimento

del Garante (provv. 11 marzo 2010 [doc. web n. 1738288]), sostenendo che l'obbligo in argomento incombeva solo in capo all'intermediario, che lo aveva assolto attraverso il proprio sito internet.

Il Tribunale ha respinto l'opposizione, osservando che i rappresentanti di commercio che si erano rivolti, in prima battuta, alla società di intermediazione intrattenevano, poi, "il contatto ed il dialogo diretto" con l'azienda che intendeva reclutarli. Nel caso di specie sussistevano quindi due distinti trattamenti e relativi distinti obblighi di informativa: l'uno, attinente all'attività di intermediazione, per la quale la società procacciatrice aveva acquisito un generico consenso preventivo; l'altro, di cui era titolare l'azienda individuale, sulla quale incombeva l'obbligo di informativa in relazione al trattamento dei *curricula* sollecitati. Il Tribunale ha pure ricordato che il Garante aveva già chiarito tale aspetto con il provvedimento del 10 gennaio 2002 [doc. web n. 1064553] (sentenza n. 126 del 27 ottobre 2010).

Trattamento dei dati in ambito giornalistico

Con sentenza n. 10971 del 22 novembre 2012 il Tribunale di Padova ha respinto l'opposizione di una società editrice in relazione alla pubblicazione di due articoli giornalistici, l'uno relativo a un furto nell'appartamento dell'interessato, l'altro all'aggressione subita dal medesimo, nella sua qualità di controllore della società che gestisce il trasporto pubblico urbano, da parte di un passeggero.

Il Garante aveva ordinato alla società di astenersi da qualsiasi ulteriore trattamento di alcune informazioni relative all'interessato -nominativo per esteso e indirizzo completo di residenza- in violazione del principio di essenzialità dell'informazione (provv. 26 ottobre 2011 [doc. web n. 1855372]).

Pur riconoscendo l'interesse pubblico dei fatti narrati, il Tribunale ha confermato che la divulgazione dell'identità della vittima "non aggiungeva alcuna utilità per i lettori", tenuto conto, altresì, che si trattava di fatti di microcriminalità e che la vittima stessa non era persona nota.

Con sentenza n. 5525 del 5 aprile 2012 la Corte di Cassazione ha cassato con rinvio la sentenza del Tribunale di Milano (n. 4302 del 6 aprile 2010) che aveva confermato il provvedimento del Garante del 28 maggio 2009 [doc. web n. 1635910] con cui era stato respinto il ricorso dell'interessato volto ad ottenere il blocco del trattamento dei suoi dati

personali in relazione ad un articolo, consultabile anche in versione informatica nell'archivio storico di un noto quotidiano, in cui si dava conto del suo arresto. Il Garante aveva ritenuto che l'articolo contenesse fatti di pubblico interesse nel rispetto del limite dell'essenzialità dell'informazione e aveva dichiarato infondata l'opposizione alla diffusione *online* dei dati, resi reperibili anche attraverso i comuni motori di ricerca.

La Suprema Corte ha statuito che il titolare dell'organo di informazione che, avvalendosi di un motore di ricerca, memorizza la notizia anche nella rete internet, è tenuto in particolare a garantire la contestualizzazione e l'aggiornamento della notizia oggetto di informazione e di trattamento, a tutela dell'interessato, nonché a salvaguardia del diritto del cittadino utente di ricevere una completa e corretta informazione. La Corte ha quindi disposto che il titolare dell'organo di informazione predisponga un sistema idoneo a segnalare, nel corpo o a margine della notizia, lo sviluppo della vicenda -nella specie, la sua definizione in via giudiziaria-, consentendone il rapido ed agevole accesso da parte degli utenti con modalità operative stabilite, in mancanza di accordo tra le parti, dal giudice di merito (cfr. *supra* paragrafi 9.5. e 18.5.).

Cessione di contratto di mutuo

È stato confermato il provvedimento del 24 settembre 2009 [doc. web n. 1657686] con cui il Garante aveva accolto il ricorso di un cittadino che aveva chiesto alla sua banca di accedere ai sensi dell'art. 7 del Codice ai suoi dati personali concernenti un contratto di mutuo stipulato con l'istituto e poi ceduto ad altra società per incorporazione. Nel ritenere legittimo l'ordine dell'Autorità di porre a disposizione del ricorrente tutta la documentazione contenente i dati, il Tribunale ha in particolare sottolineato che la disciplina sulla cessione in blocco di rapporti giuridici deve in ogni caso salvaguardare i diritti del "cliente-contraente", per cui la società incorporante "*diviene l'unico titolare del trattamento dei dati personali dei clienti delle società incorporate, proseguendo in tutti i rapporti attivi e passivi delle medesime e ha l'obbligo, quindi, di trasmettere i dati personali dei clienti in suo possesso*" (Trib. di Roma, sentenza n. 13592 del 22 giugno 2011).

Mancanza di interpello preventivo

È stata ritenuta corretta la decisione con cui il Garante ha dichiarato inammissibile, per difetto dei presupposti richiesti dall'art. 146 comma 1, del Codice, un ricorso non preceduto dall'interpello preventivo del titolare del trattamento, ritenendo non sussistente il "pregiudizio

imminente e irreparabile" che sarebbe derivato alla ricorrente dal decorso del breve termine previsto dall'art. 146, comma 2, del Codice (provv. 21 ottobre 2010 [doc. web n. 1768206]; Trib. di Milano, sentenza n. 1805 del 21 febbraio 2012).

Test di personalità

Anche il provvedimento del 21 luglio 2011([doc. web n. 1825852] v. Relazione 2011 p. 125) con il quale il Garante ha dichiarato illecita la somministrazione di questionari di personalità contenenti domande su aspetti anche molto intimi della sfera personale, ai candidati per la selezione di un dirigente tecnico, è stato pienamente confermato con due distinte sentenze: la prima ha rigettato il ricorso dell'azienda committente (Trib. di Brescia, sentenza n. 2515 del 18 luglio 2012), la seconda ha rigettato la domanda della società incaricata della selezione (Trib. di Milano, sentenza n. 12254 del 6 novembre 2012).

Le pronunce sono state emesse dai due Tribunali territorialmente competenti in funzione dei diversi luoghi di residenza dell'azienda e della società titolari del trattamento (art. 152, comma 2, del Codice, sostituito dall'art. 10, comma 2, d.lgs. n. 150/2011).

Deposito di dati in giudizio

Due sentenze hanno riguardato il deposito in giudizi civili di documenti contenenti dati personali; in particolare, rispettivamente, di un'attestazione di un istituto previdenziale sulla titolarità di una provvidenza economica per minorati civili e di documentazione bancaria.

Nel primo caso il Garante, con provvedimento del 19 giugno 2008 [doc. web n. 1542493], aveva dichiarato inammissibile il ricorso dell'interessato che lamentava di non avere autorizzato la produzione dei suoi dati sensibili, in quanto il trattamento era stato effettuato da una persona fisica per fini esclusivamente personali (art. 5, comma 3, del Codice). Nel secondo il Garante, interpellato con un reclamo, aveva respinto la richiesta di blocco del trattamento (nota 20 gennaio 2011), non essendo richiesto il consenso dell'interessato ove il trattamento sia finalizzato a far valere o difendere un diritto in sede giudiziaria e perché spetta comunque all'autorità giudiziaria decidere in merito ai dati personali versati in giudizio (art. 160, comma 6, del Codice).

In entrambi i casi le decisioni dell'Autorità sono state confermate.

Più in dettaglio, il Tribunale di Foggia, sezione distaccata di S. Severo, ha statuito che la disciplina generale in materia di trattamento di dati personali viene, anche in merito al consenso, derogata dalle disposizioni processuali ove si tratti di far valere un diritto in

giudizio, mentre il Tribunale di Lecce ha ritenuto che la produzione dei documenti fosse legittima, non richiedendosi il consenso dell'interessato nell'esercizio del diritto di difesa, come deliberato anche dal Garante nelle "Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario" (provv. 25 ottobre 2007, in G.U. 23 novembre 2007, n. 273 [doc. web n. 1457247]) (sentenza n. 169 del 17 dicembre 2012; sentenza n. 374 del 10 febbraio 2012).

Utilizzo del nome su *forum* e *blog*

Una sentenza ha riguardato la richiesta dell'interessato di ordinare al gestore di un motore di ricerca e ai titolari di due siti internet di cessare dall'utilizzo, ritenuto pregiudizievole, del proprio nome in messaggi apparsi su alcuni *forum* e *blog*. Il Garante con provvedimento del 4 novembre 2010 [doc. web n. 1774912] aveva dichiarato inammissibile il ricorso, ai sensi dell'art. 148, comma 1, lett. *b)*, del Codice, per difetto del presupposto del pregiudizio imminente e irreparabile che, come richiesto dall'art. 146, comma 1, consente di presentare il ricorso in via di urgenza, senza il preventivo interpello del titolare del trattamento. Il tribunale ha confermato la decisione, rilevando che alla data di presentazione del ricorso il lamentato pregiudizio si era già verificato (sentenza n. 1806 del 14 febbraio 2012). Il tribunale ha peraltro argomentato anche nel merito, rilevando come i titolari di domini internet non possono essere considerati titolari del trattamento, non essendo normativamente previsto a loro carico né un obbligo di controllo preventivo sui messaggi e sugli interventi degli utenti nell'area di discussione messa a loro disposizione, né di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite (art. 17 d.lgs. n. 70/2003).

Pubblicazione su internet degli elenchi nominativi dei contribuenti

Una vertenza ha avuto ad oggetto la divulgazione su internet, da parte dell'Agenzia delle entrate, dei nomi e dei redditi di tutti i contribuenti italiani per l'anno 2005.

Con provvedimento del 6 maggio 2008 [doc. web n. 1512255] il Garante aveva vietato all'Agenzia l'ulteriore divulgazione dei dati, perché in violazione della normativa all'epoca vigente (art. 69 d.P.R. n. 600/1973 e art. 19 l. n. 413/1991), che consentiva solo la distribuzione degli elenchi agli uffici delle imposte territorialmente competenti e il deposito per la consultazione presso i singoli comuni di residenza dei contribuenti.

Il Tribunale di Roma ha confermato la piena legittimità del provvedimento del Garante. Dopo aver rilevato l'evidente diversità tra la diffusione degli elenchi a livello locale e la

divulgazione su tutto il territorio nazionale, il giudice ha osservato che, comunque, non era stata data agli interessati la preventiva informativa di tale diffusione, richiesta dall'art. 13 del Codice.

Il Tribunale ha poi rilevato che il sopravvenuto d.l. n. 112/2008 (convertito con l. 113/2008), che con l'art. 42 ha rideterminato le modalità di consultazione degli elenchi, non può sanare il pregresso operato dell'amministrazione finanziaria, sia in quanto ha testualmente ad oggetto non l'attività di "diffusione" dei dati da parte dell'Agenzia, ma solo la loro "consultazione" da parte di chi ne avesse preso visione a seguito della loro diffusione in rete, sia perché, in mancanza di esplicita previsione, non può riconoscersi a tale disposizione efficacia retroattiva.

Il Tribunale ha anche respinto, per difetto di legittimazione attiva, la domanda di risarcimento dei danni cagionati ai contribuenti dalla diffusione dei dati, proposta dal Codacons nei confronti dell'Agenzia (sentenza n. 1587 del 25 gennaio 2013).

Pubblicazione di dati sull'albo pretorio di un comune

È giunta a conclusione la controversia concernente la diffusione di dati personali da parte di un comune attraverso l'affissione sull'albo pretorio dell'avviso di convocazione del consiglio comunale e della conseguente deliberazione. Il Garante aveva parzialmente accolto il ricorso dell'interessata, benché la pubblicazione sull'albo pretorio dell'avviso di convocazione del consiglio comunale fosse consentita dalla legge (d.lgs. n. 267/2000, recante il testo unico dell'ordinamento degli enti locali), ritenendo l'indicazione del nominativo dell'interessata, cui erano riferibili i dati contenuti nel documento, eccedente e non proporzionata (ai sensi dell'art. 9 della l. n. 675/1996, all'epoca vigente) rispetto alle finalità di trasparenza e di informazione perseguite (provv. 9 dicembre 2003 [doc. web n. 1054649]).

Sia il Tribunale di Messina (sentenza n. 2094 del 16 novembre 2005) che la Corte di Cassazione (sentenza n. 12726 del 20 luglio 2012) hanno confermato la decisione dell'Autorità.

Infine, si è già riferito nella parte relativa ai profili procedurali (cfr. *supra* par. 19.2.) sia della sentenza con la quale il Giudice di pace di Milano ha affermato la propria competenza funzionale e territoriale in una vertenza in materia di protezione dei dati personali (sentenza n. 100.029 del 7 gennaio 2013) sia del d.P.R. del 29 ottobre 2012, adottato su conforme

parere n. 170/2011 della Sezione prima del Consiglio di Stato, che ha dichiarato inammissibile il ricorso al Presidente della Repubblica nella stessa materia, devoluta alla giurisdizione esclusiva e funzionale dell'autorità giudiziaria ordinaria.

19.5. L'INTERVENTO DEL GARANTE NEI GIUDIZI RELATIVI ALL'APPLICAZIONE DEL CODICE

Conformemente agli indirizzi giurisprudenziali e al parere in argomento espresso dall'Avvocatura generale dello Stato -che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni- il Garante ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente pronunce dell'Autorità, ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto.

In questo quadro, l'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione degli esiti.

20. L'attività ispettiva e le sanzioni

20.1. La programmazione dell'attività ispettiva

L'attività ispettiva è lo strumento istruttorio necessario per accertare *in loco* situazioni di fatto che devono essere oggetto di valutazione da parte dell'Autorità in relazione a specifici casi. Essa però è spesso utilizzata anche con lo scopo di acquisire conoscenze in relazione a fenomeni nuovi, in vista di una successiva regolazione da parte del Garante attraverso i cd. "provvedimenti generali".

Le ispezioni eseguite nel 2012 sono state 395, disposte sulla base di programmi ispettivi semestrali le cui linee di indirizzo (ambiti del controllo e obiettivi numerici da conseguire) sono stabilite dal Collegio attraverso delibere di programmazione, rese pubbliche sul sito dell'Autorità (v. *newsletter* n. 355 del 29 febbraio 2012 e n. 361 del 22 agosto 2012).

Nel 2012, il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva fosse indirizzata ad accertamenti relativi a trattamenti di dati personali effettuati da:

- enti previdenziali mediante i propri sistemi informativi;

- soggetti che svolgono attività di *marketing* telefonico tramite *call center*, anche mediante l'utilizzo di sistemi automatizzati;

- società che forniscono servizi informatici in modalità *cloud computing*, *hosting*, *housing*, e *facility management*.

Con riferimento, invece, al secondo semestre (luglio-dicembre), oltre alla prosecuzione dei controlli nei confronti degli enti previdenziali e delle predette società che effettuano attività di *marketing*, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di trattamenti di dati effettuati:

- dall'amministrazione finanziaria mediante il sistema informativo della fiscalità (cd. "Anagrafe tributaria");

- nell'ambito della gestione di sistemi di *mobile payment*;

- nell'ambito dei sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità dei pagamenti (cd. "centrali rischi").

Più in generale, nel periodo di riferimento sono state anche effettuate nei confronti di soggetti sia pubblici sia privati verifiche:

- sull'adozione delle misure minime di sicurezza nel trattamento di dati sensibili;

- sull'adempimento dell'obbligo di notificazione da parte di soggetti individuati mediante raffronto con il Registro generale dei trattamenti;

- sulla liceità e correttezza dei trattamenti di dati personali, con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nonché alla durata della conservazione dei dati, nei confronti di soggetti appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone.

20.2. LA COLLABORAZIONE CON LA GUARDIA DI FINANZA

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto riferito nel dettaglio nelle precedenti edizioni (cfr., da ultimo, Relazione 2009 p. 240 e ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente a effettuare la gran parte degli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge.

Laddove emergano violazioni penali o amministrative, la Guardia di finanza provvede direttamente a informare l'autorità giudiziaria competente e a formalizzare la contestazione delle sanzioni amministrative accertate.

In tal modo l'Autorità dispone di un dispositivo di controllo flessibile ed articolato che integra l'attività svolta direttamente dal Dipartimento ispettivo dell'Autorità e che consente di espletare verifiche sul territorio in modo efficace e tempestivo.

Nel quadro dell'attività di formazione sono stati organizzati quattro corsi presso la Scuola

di polizia tributaria, denominati "Collaborazione della Guardia di finanza con l'Autorità Garante per la protezione dei dati personali", diretti a illustrare al personale operante nei reparti territoriali del Corpo i princìpi del Codice e le prassi operative sui controlli in materia di *privacy*. Circa ottanta, tra ufficiali ed ispettori, hanno partecipato a tali attività.

Sono stati inoltre organizzati due seminari di approfondimento presso il Nucleo speciale *privacy*: il primo sugli aspetti *privacy* legati all'utilizzo di sistemi di videosorveglianza o di altre tecnologie in ambienti di lavoro e il loro eventuale impatto sul controllo a distanza dei lavoratori; il secondo dedicato all'analisi delle norme introdotte nel Codice a seguito del recepimento della Direttiva n. 136/2009 (d.lgs. 28 maggio 2012, n. 69) e delle nuove disposizioni sull'uso dei cd. "*cookie*".

20.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

I settori più significativi nell'ambito dei quali è stata effettuata l'attività ispettiva nel 2012 sono:

- enti pubblici (centri per l'impiego, regioni, province e comuni), con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza (n. 44);

- società che erogano servizi alle persone (prenotazioni crociere e ristrutturazioni edilizie), con particolare riferimento all'utilizzo dei dati dei clienti acquisiti via web (n. 32);

- società che acquistano da privati e commercializzano gioielli e oggetti preziosi di varia natura (cd. "compro oro"), con riferimento al trattamento dei dati personali dei clienti (n. 30);

- ospedali pubblici e cliniche private, con riferimento alla liceità dei trattamenti dei dati sulla salute dei pazienti e all'adozione delle misure di sicurezza (n. 29);

- società di noleggio nautico che raccolgono i dati personali degli interessati via web (n. 27);

- società che forniscono preventivi *online* di polizze assicurative, mutui e servizi finanziari in genere (n. 26);

- società editoriali, con riferimento alla liceità del trattamento dei dati dei clienti acquisiti nell'ambito delle richieste di abbonamento ai quotidiani *online* (n. 26);

- soggetti privati che acquisiscono dati personali nell'ambito di selezioni del personale effettuate mediante la pubblicazione di annunci su riviste o siti specializzati (n. 18);

- società che effettuano attività di *marketing* anche fornendo a terzi servizi di *call center*, con riferimento alla liceità dei dati utilizzati per l'attività di *marketing*, nonché alle modalità con le quali viene assicurato il rispetto dei diritti dell'interessato (n. 17);

- società che gestiscono catene di grande distribuzione, con riferimento al trattamento dei dati personali di clienti e dipendenti acquisiti mediante sistemi di videosorveglianza (n. 16);

- fornitori di servizi di comunicazione elettronica accessibili al pubblico (*internet service provider*), per verificare il rispetto delle disposizioni sulla conservazione dei dati di traffico telefonico e telematico per finalità di accertamento dei reati (cd. "*data retention*") (n. 13);

- società e/o enti che utilizzano sistemi di localizzazione satellitare, con riferimento al rispetto dei diritti dei dipendenti previsti dal Codice e dallo Statuto dei lavoratori (n. 10);

- società fornitrici di energia elettrica e gas, con riferimento all'utilizzo dei dati dei clienti (n. 8);

- società telefoniche, istituti bancari ed emittenti di carte di credito che forniscono servizi di *mobile payment,* in relazione alla tipologia e ai flussi dei dati personali che si determinano con l'uso dei dispositivi da parte dei clienti (n. 5);

- enti pubblici e/o società che detengono banche dati di pazienti nefropatici cronici, a seguito dell'istituzione del registro italiano di dialisi e trapianto (n. 4);

- società che gestiscono banche dati relative ai sistemi di informazione creditizia, con riferimento alla liceità della raccolta dei dati dei soggetti nei cui confronti svolgono la propria attività (n. 4);

- società e/o enti pubblici che utilizzano i sistemi informativi della fiscalità (Anagrafe tributaria) in relazione al parere che l'Autorità ha reso all'Agenzia delle entrate relativamente al trasferimento dei dati bancari nel sistema informativo della fiscalità (n. 3).

A questi si aggiungono controlli effettuati nei confronti di specifici titolari del trattamento per esigenze istruttorie connesse alle segnalazioni/reclami pervenuti all'Autorità.

Da questi dati emergono le seguenti linee di azione dell'attività di controllo nel 2012:

- verifica del livello di attuazione delle disposizioni del Codice in ambito pubblico, con particolare attenzione all'adozione delle misure di sicurezza in relazione alla crescita dei volumi dei flussi informativi in formato elettronico, all'interconnessione delle banche dati pubbliche ed al sempre maggiore utilizzo del web per la fornitura dei servizi ai cittadini;

- controllo sulle modalità di raccolta dei dati personali da parte di soggetti privati nell'ambito della fornitura di servizi o dell'acquisto di beni *online*, con particolare riferimento al rispetto degli obblighi informativi previsti dal Codice e all'accertamento della correttezza delle procedure di acquisizione del consenso degli interessati;

- accertamento del rispetto degli adempimenti *privacy* da parte degli organismi sanitari pubblici e privati, con particolare riferimento ai dati sulla salute trattati anche mediante nuovi servizi di consultazione della documentazione clinica in formato digitale (cd. "*dossier* sanitario elettronico");

- contrasto al fenomeno del cd. "*marketing* selvaggio" effettuato utilizzando illecitamente dati personali (prevalentemente numeri di telefono fissi e mobili) di cittadini, senza aver acquisito il loro consenso o in violazione della loro volontà di non essere disturbati, espressa mediante iscrizione della loro utenza al Registro pubblico delle opposizioni (attività che ha avuto i suoi effetti anche in ambito sanzionatorio come riportato nel successivo par. 20.4.2.).

In relazione a quanto emerso dagli accertamenti ed alle conseguenti proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, l'Autorità ha emesso alcune deliberazioni particolarmente significative, tra le quali, oltre a quelle già riportate nella Relazione 2011, si segnalano:

- divieti di trattare dati biometrici in violazione dei princìpi di necessità, liceità e proporzionalità previsti dagli artt. 3 e 11, del Codice a:

a) società che gestiscono palestre, che li utilizzavano per consentire l'accesso dei clienti alle proprie strutture e servizi (provv.ti 16 febbraio 2012 [doc. web n. 1894570] e 29 marzo 2012 [doc. web n. 1891999]);

b) imprese appaltatrici, che utilizzavano i dati biometrici delle maestranze per regolarne l'accesso al cantiere (provv. 13 settembre 2012 [doc. web n. 1927456]);

- il parere reso dal Garante all'Agenzia delle entrate sulle modalità di trasmissione e di conservazione dei dati contabili all'Anagrafe tributaria da parte di banche e operatori finanziari (provv. 17 aprile 2012 [doc. web n. 1886775]);

- il provvedimento con il quale è stato prescritto a una società di vigilanza di fornire ai lavoratori una compiuta informativa ai sensi degli artt. 11, comma 1, lett. *a)* e 13 del Codice

con riguardo al trattamento dei dati personali effettuati mediante il sistema di localizzazione, nonché di collocare all'interno dei veicoli aziendali vetrofanie recanti la dizione "veicolo sottoposto a localizzazione" o comunque un avviso ben visibile che segnali la possibilità di geolocalizzare il mezzo (provv. 1° agosto 2012 [doc. web n. 1923293]);

- il provvedimento con il quale è stato dichiarato illecito il trattamento dei dati riferiti ai lavoratori consistente nella registrazione e riascolto delle telefonate effettuate dagli operatori di un *call center*, nonché nell'attività di monitoraggio della condotta tenuta dagli operatori stessi effettuato mediante l'analisi del numero e della durata delle conversazioni intercorse tra i dipendenti e i clienti (provv. 1° agosto 2012 [doc. web n. 1923325]);

- i provvedimenti con il quale è stato vietato il trattamento dei dati personali dei dipendenti di una società, effettuato a mezzo del sistema di videosorveglianza collocato all'interno dell'azienda nonché mediante apparati di rilevazione dell'audio in quanto in violazione dei princìpi di liceità, pertinenza e non eccedenza previsti dall'art. 11 del Codice e di quanto previsto dall'art. 4 dello Statuto dei lavoratori (provv.ti 4 ottobre 2012 [doc. web n. 2066968] e 25 ottobre 2012 [doc. web n. 2212826]);

- il provvedimento con il quale è stato vietato il trattamento di dati personali posto in essere da una società in relazione all'invio di proposte commerciali via posta cartacea ed elettronica, alla comunicazione di dati a terzi nonché all'acquisizione degli stessi dati tramite gli inserti pubblicitari su riviste, senza aver rilasciato un'idonea informativa ai sensi dell'art. 13 e senza che risultasse la prova del consenso preventivo, specifico e informato degli interessati ai sensi degli artt. 23 e 130, del Codice (provv. 11 ottobre 2012 [doc. web n. 2089777]);

- il provvedimento con il quale l'accesso, tramite il sistema di protocollo informatico di un ente pubblico, alle pratiche contenenti dati personali dei dipendenti, è stato limitato al solo personale, previamente formato, incaricato della gestione dei dati dei dipendenti stessi (provv. 11 ottobre 2012 [doc. web n. 2097560]);

- il provvedimento con cui è stata esaminata la correttezza delle misure adottate da un ente pubblico per prevenire la conoscibilità ingiustificata di dati personali dei dipendenti nell'ambito dei procedimenti amministrativi collegati alla gestione del personale (provv. 18 ottobre 2012 [doc. web n. 2174351]);

- il provvedimento con il quale è stato dichiarato illecito il trattamento di dati personali effettuato da una società privata mediante un sistema di videosorveglianza che riprendeva aree esterne e interne agli esercizi commerciali per finalità di pubblica sicurezza (provv. 25 ottobre 2012 [doc. web n. 2212623]).

In molti dei casi sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha avviato anche un procedimento sanzionatorio; in altri, rilevando condotte penalmente rilevanti, ha trasmesso gli atti alla competente procura della Repubblica.

20.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

20.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

Nel 2012, in relazione alle istruttorie effettuate, sono state inviate n. 56 segnalazioni di violazioni penali all'Autorità giudiziaria di cui:

- n. 23 per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;

- n. 18 per la mancata adozione delle misure minime di sicurezza;

- n. 5 per trattamento illecito dei dati;

- n. 3 per falsità nelle dichiarazioni e notificazioni al Garante;

- n. 1 per inosservanza di un provvedimento del Garante;

- n. 6 in relazione ad altre violazioni penali.

Rispetto agli anni precedenti si è avuta una maggiore incidenza dell'accertamento di violazioni penali connesse allo Statuto dei lavoratori, la cui disciplina relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8) è esplicitamente fatta salva dal Codice (artt. 113 e 114), ed è munita delle sanzioni previste dall'art. 171.

L'aumento dell'accertamento delle violazioni penali in questo settore dipende:

- dalle numerose segnalazioni di presunte violazioni presentate all'Autorità dai lavoratori o dai sindacati;

- dalla costituzione nell'Autorità, a partire dall'aprile del 2011 (v. Relazione 2011 p. 117) di una unità organizzativa con competenze in materia di lavoro pubblico e privato.

Rimangono tuttavia numerose le violazioni delle misure minime di sicurezza nonostante il d.l. 9 febbraio 2012, n. 5 (convertito, con modificazioni, dalla l. 4 aprile 2012, n. 35) abbia abrogato l'adempimento relativo alla tenuta di un aggiornato documento programmatico sulla sicurezza (dps).

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone, almeno potenzialmente, i dati personali degli interessati all'accesso da parte di persone non autorizzate e a trattamenti non consentiti, intaccando il naturale affidamento degli interessati nei confronti del titolare del trattamento.

Sotto il profilo procedurale, nel caso in cui venga rilevata una violazione di una o più misure minime di sicurezza (specificatamente previste dal disciplinare tecnico sulle misure di sicurezza Allegato B. del Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della predetta violazione e, verificato il ripristino delle misure violate, ammette il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento della prescrizione ed il pagamento della somma vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

20.4.2. Sanzioni amministrative

A seguito delle ispezioni effettuate e delle istruttorie curate dall'Ufficio, sono stati avviati n. 578 procedimenti sanzionatori amministrativi.

Le violazioni accertate hanno riguardato:

- omessa o inidonea informativa, art. 161 (n. 258);

- trattamento illecito amministrativo, art. 162, comma 2-*bis* (n. 183);

- utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing*, art. 162, comma 2-*quater* (n. 64);

- omessa informazione o esibizione al Garante, art. 164 (n. 20);

- omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice, art. 162, comma 2-*bis* (n. 17);

- inosservanza di un provvedimento del Garante, art. 162, comma 2-*ter* (n. 17);

- omessa o incompleta notificazione, art. 163 (n. 13);

- sanzioni in materia di conservazione dei dati di traffico, art. 162-*bis* (n. 3);

- banche dati di particolare rilevanza e dimensioni, art. 164-*bis*, comma 2 (n. 3).

Con riferimento alle suddette 183 violazioni di cui all'art. 162, comma 2-*bis* "trattamento illecito amministrativo", occorre precisare che la disposizione prevede una sanzione pecuniaria, da 10.000 a 120.000 euro in relazione alla violazione delle eterogenee disposizioni indicate nell'art. 167 del Codice, quali gli artt. 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposizioni concernenti il trattamento dei dati da parte di soggetti pubblici), 23, 25, 26, 27 (disposizioni concernenti il trattamento dei dati da parte dei soggetti privati), 45 (trasferimenti all'estero vietati), 123, 126, 129 e 130 (disposizioni specifiche per le comunicazioni elettroniche).

Nel 2012 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato le seguenti fattispecie:

- violazione del consenso dell'interessato in rapporto agli artt. 23 e 130, del Codice (n. 126);

- violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati non sensibili senza i necessari presupposti di legge o regolamento) (n. 36);

- violazioni commesse da enti pubblici con riferimento a dati sensibili (n. 13);

- violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice (n. 5);

- violazioni commesse da soggetti privati in relazione al trattamento di dati sensibili o giudiziari (n. 3).

Da questi dati si può rilevare che:

- in senso assoluto, anche per quest'anno, il maggior numero di violazioni accertate ha riguardato l'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali. Questo

elemento si spiega alla luce del fatto che l'obbligo di informativa costituisce l'adempimento più generale previsto dal Codice;

- al secondo posto si colloca il "trattamento illecito amministrativo";

- infine, sommando le violazioni del consenso dell'interessato (n. 126) a quelle relative all'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni (n. 64) si arriva ad un totale di 190 violazioni commesse da soggetti privati che hanno utilizzato i dati personali degli interessati senza (o contro) la volontà di quest'ultimi. Si tratta principalmente di trattamenti effettuati da aziende per finalità di *marketing* (cd. "*marketing* selvaggio") (cfr. *supra* par. 11.).

I procedimenti sanzionatori definiti con ordinanza dall'Autorità sono stati 194. Di questi 118 hanno comportato l'applicazione di una sanzione e 76 si sono invece conclusi con l'archiviazione, in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era a lei imputabile.

Tra le ordinanze più rilevanti adottate si segnalano quelle nei confronti di due importanti società in relazione all'utilizzo illecito di ingenti banche dati per finalità di *marketing* [doc. web nn. 2115627 e 2368171]. In questi due casi ha trovato per la prima volta applicazione la sanzione prevista dall'art. 164-*bis*, comma 2, in cui è previsto che per più violazioni delle disposizioni contenute nel Titolo III, Capo I, del Codice, in relazione a banche dati di particolare rilevanza o dimensioni, non è ammesso il pagamento in misura ridotta.

Le ordinanze evidenziano che l'illecito configura una "fattispecie complessa", collegata ma autonoma rispetto a quelle presupposte, tra le quali ricorrono, nel caso di specie, quelle di cui agli artt. 161, 162, comma 2-*bis* e 162, comma 2-*ter*. La violazione di cui all'art. 164-*bis*, comma 2, è infatti punita con una sanzione quantificabile autonomamente. Inoltre, il procedimento sanzionatorio che si instaura con la contestazione della violazione di cui all'art. 164-*bis*, comma 2, si differenzia da quello relativo alle altre violazioni per l'inapplicabilità dell'art. 16, l. n. 689/1981 in tema di pagamento in misura ridotta. Già nella sua struttura formale, l'art. 164-*bis*, comma 2, ha pertanto le caratteristiche tipiche della fattispecie sanzionatoria autonoma (condotta e sanzione pecuniaria prevista tra un minimo e un massimo). La norma *de quo* infatti tutela un bene giuridico ulteriore e diverso rispetto a

quello offeso dalle singole violazioni presupposte, poiché è specifica la lesione che si determina ai diritti quando dette plurime violazioni riguardano non singoli dati ma, come nel caso di specie, una banca dati "*di particolare rilevanza e dimensioni*".

Complessivamente le entrate relative all'attività sanzionatoria, per l'anno 2012, sono state pari a 3.769.217 euro in relazione a pagamenti effettuati:

- spontaneamente dai contravventori (2.928.267 euro);

- a seguito di ordinanza-ingiunzione adottata dall'Autorità (780.950 euro);

- a seguito di ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (60.000 euro).

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e sono utilizzati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

20.4.3. Le sanzioni amministrative introdotte nel Codice con il d.lgs. 28 maggio 2012, n. 69

Come più ampiamente riportato (cfr. *supra* 2.1.), per effetto del recepimento della Direttiva europea n.136/2009/CE avvenuto con il d.lgs. 28 maggio 2012, n. 69, sono state introdotte nuove disposizioni nel Codice, in particolare con riferimento alle comunicazioni elettroniche e alle cd. "violazioni di dati" o *data breach*.

La nuova disciplina ha previsto una serie di adempimenti che i fornitori di servizi di comunicazione elettronica accessibili al pubblico devono attuare nel caso accertino che i dati personali contenuti nei loro sistemi siano stati violati.

È importante osservare che la nuova disciplina riguarda al momento solo quei soggetti che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti "*nella trasmissione di segnali su reti di comunicazioni elettroniche*" (art. 4, comma 2, lett. *d)* ed *e),* del Codice), anche se nell'ambito della revisione della disciplina comunitaria si prevede una sua estensione agli altri settori.

Il mancato rispetto degli adempimenti comporta l'applicazione delle sanzioni previste dall'art. 162-*ter,* anch'esso introdotto dal d.lgs. n. 69/2012.

Tali sanzioni sono destinate solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ma se l'erogazione dei predetti servizi è stata affidata a terzi (caso tipico è l'*outsourcer* informatico che gestisce i sistemi informativi attraverso i quali il fornitore stesso eroga i servizi ai propri clienti) anche questi sono soggetti alle sanzioni ove non abbiano comunicato "*senza indebito ritardo*", al fornitore, le informazioni necessarie ai fini di porre in essere gli adempimenti di competenza (art. 162-*ter*, comma 5).

Le condotte sanzionate riguardano:

- l'omessa (o tardiva) comunicazione della violazione di dati personali al Garante;

- l'omessa (o tardiva) comunicazione della violazione di dati personali al contraente o altra persona, quando dovuta (ovvero quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona e il fornitore non ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione);

- la tenuta di un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni in materia.

Il regime sanzionatorio previsto dal legislatore è particolarmente severo:

- da 25.000 a 150.000 euro, in caso di violazione dell'obbligo di comunicazione al Garante;

- da 150 a 1.000 euro per ciascun contraente o altra persona nei cui confronti tale comunicazione venga omessa o ritardata.

L'apparente tenuità della sanzione non deve ingannare in quanto molto spesso, quando si verifica una violazione dei dati personali contenuti in una banca dati, la stessa può riguardare centinaia, migliaia e talvolta anche decine o centinaia di migliaia di interessati. Nel caso quindi si accerti che a fronte di una violazione dei dati che ha riguardato ad esempio mille persone, un fornitore di servizi di comunicazione elettronica abbia omesso di effettuare le comunicazioni dovute agli interessati, l'importo della pena pecuniaria sarà moltiplicato per mille.

È stata inoltre espressamente esclusa l'applicazione dell'art. 8, l. n. 689/1981, che prevede, in caso di violazione di diverse disposizioni o di più violazioni della stessa disposizione l'applicazione della sanzione prevista per la violazione più grave, aumentata sino al triplo.

Per evitare un'eccessiva afflittività della sanzione nei casi più gravi, il legislatore ha comunque stabilito che la sanzione amministrativa commisurata al numero delle omesse comunicazioni agli interessati non può essere applicata in misura superiore al 5% del volume d'affari realizzato dal soggetto sanzionato nell'ultimo esercizio chiuso anteriormente alla notificazione della contestazione della violazione amministrativa.

21. Le relazioni internazionali

Si premette che in questa sezione si riferisce in merito ad attività aventi intensità ed effetti nettamente differenziati, in quanto il graduale assorbimento di competenze normative statali da parte delle Istituzioni europee, nel progressivo instaurarsi di un quadro ordinamentale sempre più tendente all'unità, comporta un impegno che, oltre al settore preposto alle relazioni internazionali, coinvolge le diverse strutture dell'Autorità, quali, solo per citarne alcune, quelle competenti in materia di tecnologie, comunicazioni elettroniche, trattamenti di dati in internet, trasferimento di dati a Paesi terzi, *cloud computing*.

In questi ambiti il ruolo del Garante è quello di una Autorità nazionale chiamata, insieme con gli omologhi degli altri Paesi UE ad interpretare, intervenire e talvolta a risolvere conflitti applicativi o approcci diversi su questioni di comune interesse tra i Garanti dei diversi Stati membri.

Ciò vale anche, dopo l'entrata in vigore del Trattato di Lisbona, non solo per i trattamenti di dati che si svolgono nei settori "disciplinati" dalle disposizioni delle Direttive nn. 95/46/CE e 136/2009/CE per il settore delle comunicazioni elettroniche, che costituiscono il quadro armonizzato a livello europeo dei princìpi di protezione dei dati personali, per i quali la "stanza di compensazione" oltre che di cooperazione è oggi il Gruppo istituito ai sensi dell'Art. 29 della Direttiva n. 95/46/CE per svolgere i compiti più specificamente descritti nell'art. 30 di quest'ultima, ma anche per la cooperazione nel settore in precedenza denominato "trattamenti di polizia e giustizia".

Le analisi e le decisioni prese nei consessi comunitari sono sempre più rilevanti, se non anche vincolanti, per le autorità ed in tal senso, come vedremo, il pacchetto di riforma del quadro giuridico europeo in materia di protezione dei dati personali presentato dalla Commissione europea il 25 gennaio 2012 contiene ulteriori espliciti obblighi.

Ne deriva una crescente importanza delle attività svolte nel settore, l'intensificarsi di impegni a Bruxelles e l'esigenza di integrare nelle priorità di lavoro quelle provenienti dalle decisioni comuni, che richiede e richiederà sempre più in futuro la disponibilità di risorse finanziarie e di personale specificamente formato (con conoscenze linguistiche, di diritto comunitario e

tecnologiche) per far fonte adeguatamente ai nuovi compiti ed alle nuove sfide dell'integrazione degli ordinamenti. Su questi aspetti è in corso un dialogo con la Commissione europea, per far in modo che il nuovo quadro regolamentare preveda, oltre ai princìpi, anche i mezzi per garantire il concreto ed ottimale funzionamento dei meccanismi in parola.

Altre attività, nell'ambito del Consiglio d'Europa e dell'OCSE, per quanto anch'esse onerose, si svolgono in un quadro di cooperazione con tempi e modalità più strutturati e programmabili.

21.1. LA RIFORMA DEL QUADRO GIURIDICO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

Il 2012 è stato un anno cruciale per la discussione sulla riforma globale della normativa UE in materia di protezione dei dati. Preso atto dei radicali cambiamenti che hanno riguardato il trattamento dei dati a causa dell'incessante progresso tecnologico e della globalizzazione, nonché dell'esigenza di garantire una maggiore uniformità applicativa dei princìpi *privacy* nei 27 Stati membri (v. Relazione 2011 p. 190 e ss.) la Commissione, il 25 gennaio 2012, ha presentato le proposte per un nuovo quadro giuridico europeo in materia, nell'intento di rafforzare i diritti della *privacy online* e stimolare l'economia digitale europea [doc. web nn. 1895615 e 1895611]. Il pacchetto di riforma si compone di una proposta di regolamento generale sulla protezione dei dati -volta a sostituire la Direttiva n. 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali)- e di una proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (settori attualmente esclusi dal campo di applicazione della Direttiva n. 95/46/CE). Tale proposta di direttiva mira a sostituire la Decisione quadro n. 2008/977 (sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale), estendendone il campo di applicazione anche ai trattamenti "domestici" e non solo ai dati oggetto di scambio tra autorità competenti degli Stati membri.

Nella proposta di regolamento si registrano diverse novità rispetto all'odierno quadro normativo. Restano ferme le definizioni fondamentali, ma con alcune significative aggiunte (quali quelle di dato genetico e dato biometrico); viene introdotto il principio

dell'applicazione del diritto comunitario anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini europei o tali da consentire il monitoraggio dei comportamenti di cittadini UE; si stabilisce il diritto degli interessati alla cd. "portabilità del dato" (ad. es., nel caso in cui si intendesse trasferire i propri dati da un *social network* ad un altro); si introduce il cd. "diritto all'oblio", ossia il diritto ad ottenere la cancellazione delle informazioni personali anche *online*; scompare l'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito da quello di nominare un *data protection officer,* per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti; viene introdotto il requisito della valutazione dell'impatto-*privacy* (*privacy impact assessment*) oltre al principio generale cd. "*privacy by design*" (cioè la previsione di misure a protezione dei dati già al momento della progettazione di un prodotto o di un *software*); si stabilisce l'obbligo per tutti i titolari di notificare all'autorità competente le violazioni dei dati personali (*personal data breach*); si fissano più specificamente poteri (anche sanzionatori) e requisiti di indipendenza delle Autorità nazionali di controllo, il cui parere sarà indispensabile qualora si intendano adottare strumenti normativi rilevanti per la protezione dei dati.

La proposta di direttiva sui trattamenti per finalità di giustizia e di polizia riprende l'impostazione del regolamento, richiamato in molte delle sue previsioni, e contiene, tuttavia, disposizioni specifiche sulle responsabilità dei titolari e sugli obblighi che su di essi incombono in materia di trasparenza ed accesso, fissa i criteri di legittimità dei trattamenti in questione, nonché i meccanismi di mutua cooperazione ed i poteri delle Autorità nazionali di controllo.

Le due proposte che formano il cd. "pacchetto protezione dati" hanno iniziato il loro *iter* legislativo presso il Parlamento europeo ed il Consiglio dell'Unione europea.

Il Consiglio UE ha affidato il compito di analizzare e discutere il progetto di riforma ad un Comitato denominato DAPIX ("protezione dati e scambio di informazioni") che ha dato inizio alle sue attività durante la presidenza danese (primo semestre 2012) e proseguito i lavori sotto la presidenza cipriota (secondo semestre 2012) ed irlandese (primo semestre 2013).

Il Garante ha partecipato attivamente sia al Gruppo Art. 29, che riunisce le Autorità europee di protezione dei dati e che ha continuato a fornire alla Commissione ed alle altre istituzioni la propria consulenza, sia al gruppo DAPIX, in qualità di esperto nella delegazione italiana.

Il Parlamento europeo, dopo aver nominato i relatori per ciascuna delle proposte, ha elaborato numerosi emendamenti che saranno auspicabilmente votati nella Commissione per le libertà civili, la giustizia e gli affari interni (Commissione LIBE) entro la primavera del 2013, per poi essere negoziati con Consiglio e Commissione nel tentativo di raggiungere un'intesa volta all'adozione del pacchetto di riforma prima del termine del mandato del Parlamento stesso.

Nonostante il forte richiamo all'esigenza di mantenere un elevato livello di tutela -pur garantendo la semplificazione di obblighi ed oneri per i titolari di trattamento (pubblici e privati)- il testo, nella sua versione iniziale, presenta diverse ambiguità e rischi, acuiti dall'andamento dei lavori in corso presso il DAPIX e dalla forte pressione dei grandi operatori commerciali sui legislatori e sulle istituzioni nazionali.

Suscita alcune perplessità la scelta dello strumento regolamentare, direttamente ed immediatamente applicabile, le cui previsioni, in settori molto diversi tra loro che talora risentono di tradizioni nazionali radicate, specie in ambito pubblico, potrebbero portare ad un "ribasso" dei livelli di protezione attualmente assicurati dai diversi ordinamenti degli Stati membri.

Come anticipato, in materia il Gruppo Art. 29 ha pubblicato diversi documenti contenenti osservazioni anche critiche nei confronti dei due testi, e numerosi suggerimenti per la Commissione europea e le altre istituzioni coinvolte nell'*iter*. Lo stesso ha fatto il Garante europeo della protezione dati, che ha una specifica competenza a formulare pareri sulle proposte legislative.

I temi più dibattuti sono stati l'applicazione del principio dello "stabilimento principale" (*main establishment*) dell'impresa che tratti dati in più di uno Stato membro quale fondamento dello "sportello unico" (*one stop shop*), per tutti gli obblighi *privacy*, in quanto l'affermazione della competenza esclusiva dell'Autorità di protezione dati dello Stato in cui

l'impresa individua il suo stabilimento principale non terrebbe conto sufficientemente dell'indipendenza e del principio di leale collaborazione delle autorità nazionali, nonché delle specifiche esigenze legate alle garanzie degli interessati; i poteri eccessivi della Commissione europea per quanto riguarda gli atti delegati e di esecuzione (che in molti casi andrebbero a precisare elementi essenziali e non accessori dei singoli meccanismi di trattamento); la rigidità del sistema sanzionatorio che impone sanzioni pecuniarie lasciando pochi margini di flessibilità per sanzioni alternative egualmente dissuasive ed efficaci quali le misure interdittive o di blocco del trattamento.

Più in dettaglio, nel marzo 2012 con il parere (n. 1/2012 - WP 191 [doc. web n. 2375522]) il Gruppo Art. 29, pur condividendo lo spirito delle proposte adottate dalla Commissione europea in quanto tese a rafforzare la protezione dei dati degli interessati, a definire meglio le responsabilità per il trattamento e a consolidare la posizione delle autorità di controllo tanto a livello nazionale che internazionale, ha auspicato miglioramenti del testo che portino all'edificazione di un sistema di protezione più forte ed omogeneo nei diversi Stati.

Nel parere è stata rilevata la difficoltà di considerare il pacchetto di riforma come un quadro comprensivo ed unitario (obiettivo che la Commissione ha dichiarato come centrale) sia perché sono stati presentati due strumenti diversi, sia perché la proposta di direttiva, formulata in modo generico, lascia margini troppo ampi al legislatore nazionale, ciò inficiando il proclamato intento di "armonizzazione". Positivo è stato ritenuto l'inserimento sia delle disposizioni che incentivano i responsabili del trattamento ad investire, sin dall'inizio, in una corretta salvaguardia dei dati (nella protezione fin dalla progettazione e nella protezione di *default*, nonché mediante le valutazioni d'impatto sulla protezione dei dati), sia di quelle volte ad armonizzare i poteri e le competenze delle autorità di controllo. Critiche sono invece state espresse sulla compatibilità costituzionale del principio dell'*one stop shop* (v. *supra*) per i suoi effetti sulla legge applicabile e sulla giurisdizione, sull'effettività della tutela per trattamenti che si dirigono a cittadini europei svolti da soggetti non stabiliti nell'UE, sulla mancata previsione espressa dell'esigenza di dotare di risorse adeguate le autorità di protezione dati, nonché sulla debolezza del modello di cooperazione europea nel quale risulta prevalente il ruolo della Commissione.

Dopo la discussione svoltasi nel DAPIX a seguito della presentazione del parere nel maggio 2012, il Gruppo ha adottato, il 5 ottobre 2012, un secondo più specifico parere (n. 8/2012 - WP 199 [doc. web n. 2133818]) per fornire ulteriori indicazioni di merito e segnalare non solo al Parlamento UE, ma anche al Consiglio, la preoccupazione dei Garanti europei in relazione all'andamento della discussione nell'ambito dello stesso DAPIX. Il nuovo parere assume posizione su alcune questioni di fondo, quali la definizione di dato personale, le attività puramente "domestiche" (che si sottraggono all'applicazione dei princìpi di protezione dei dati), la nozione di consenso, indicando la perdurante validità delle definizioni fornite dalla Direttiva n. 95/46/CE e la necessità del loro mantenimento, suggerendo al contempo la possibilità di introdurre specifiche deroghe, laddove necessario nei singoli articoli, senza alterare le definizioni.

Il parere, seppur in modo non esaustivo, affronta anche alcune delle già ricordate questioni "orizzontali" che investono l'intera struttura del regolamento, quali l'opportunità del ricorso ad atti delegati da parte della Commissione, nei molti casi menzionati nella proposta (art. 86).

Buona parte delle preoccupazioni formulate dai Garanti sono rispecchiate nei *report* presentati dai due relatori alla Commissione LIBE del Parlamento europeo, incaricata di redigere la posizione finale sul testo. I *report* contengono diverse centinaia di emendamenti che segnalano la necessità di apportare numerosi aggiustamenti.

Nel quadro delle possibili evoluzioni che le proposte di regolamento e di direttiva potrebbero avere e le ripercussioni sull'attività delle autorità di protezione dati, si segnala anche la lettera del 4 aprile 2012 [doc. web n. 2375399] inviata alla Vicepresidente della Commissione Reding, riguardo alla menzionata mancanza di un'espressa previsione circa la necessità di dotare le autorità di protezione dati di risorse adeguate.

I prossimi mesi saranno decisivi per capire se l'ambizioso progetto della Commissione europea vedrà la luce sostanzialmente immutato nelle linee generali e, soprattutto, se sarà raccolta la sfida di una protezione dati che sia all'altezza degli sviluppi tecnologici e del nuovo quadro di diritti fondamentali introdotto nell'UE con il Trattato di Lisbona.

21.2. LE CONFERENZE DELLE AUTORITÀ GARANTI SU SCALA INTERNAZIONALE

La Conferenza internazionale delle autorità di protezione dati a Punta del Este

La 34ª Conferenza internazionale dei *Privacy Commissioners* si è svolta in Uruguay (Punta del Este) dal 23 al 24 ottobre 2012.

Nel corso della sessione aperta della Conferenza, intitolata "*Privacy and Technology in balance*", sono stati discussi in particolare l'impatto degli sviluppi della società dell'informazione e le aspettative di questa riguardo a *standard* e prassi in materia di protezione dei dati. Nell'intervento di apertura della prima sessione è stata sottolineata la necessità di nuovi ed ulteriori interventi normativi per tener conto delle conseguenze della tendenza a porre in essere infrastrutture globali volte ad ottenere un impiego ottimale delle informazioni personali, sia nel settore privato, sia in quello pubblico. A tal proposito è stata rilevata l'esigenza di rileggere i princìpi base del trattamento dei dati anche per meglio garantire i diritti della persona. In particolare si è evidenziato come nel settore pubblico il diritto individuale debba essere bilanciato con altri interessi pubblici rilevanti, mentre nel settore privato c'è una chiara tendenza a trattare i dati personali come beni (una sorta di "parte commercializzabile" della propria personalità). I grandi fornitori di servizi internet (Microsoft, Google, solo per citare i maggiori) agiscono in condizioni di quasi monopolio e non sono soggetti alle norme sulla concorrenza con conseguenti limitazioni alla libertà di scelta degli utenti. Sottolineato che in questo momento regna l'incertezza nei comportamenti dei diversi attori, è stato ribadito come compito del diritto sia, costruendo sui princìpi fondamentali, dare risposte alle nuove sfide con ciò evitando che "la tecnica faccia la regola".

La seconda sessione si è occupata di *privacy* ed *e-governement* evidenziando, anche in questo settore, il problema delle grandi raccolte di dati e degli usi "non attesi" degli stessi. È stata sottolineata la necessità di aggiornare le regole di protezione dati per una nuova amministrazione, più accessibile e vicina ai cittadini. Il tema è stato approfondito anche in sessioni parallele dedicate all'*Open Government* ed all'*e-Health.* Le altre sessioni plenarie sono state dedicate ai modelli di regolazione esistenti, per individuare le buone prassi e stimolare la cooperazione tra i diversi mondi e modelli, peraltro in evoluzione (Europa, Stati Uniti, ma anche Oriente e soprattutto America latina).

Altri temi, trattati nelle sessioni parallele, hanno riguardato la geolocalizzazione pubblica e privata, la nuove sfide del web 3.0 anche per le autorità pubbliche, le tecniche informatiche per preservare le prove (*forensic tools*), la cooperazione internazionale tra le autorità di protezione dei dati e della *privacy*, il *marketing* comportamentale *online*, l'impiego della biometria, gli "*smart data*", il consenso informato, il diritto alla tutela dei dati personali come diritto fondamentale (che ha visto come relatore il Segretario generale del Garante), le sfide nascenti dall'incontro tra lotta alla pirateria e tutela della *privacy*.

La sessione chiusa della Conferenza, la cui partecipazione è limitata alle autorità di protezione dei dati -largamente ampliata nei tempi, rispetto alle precedenti conferenze- è stata dedicata ad una cospicua presentazione del tema "profilazione", con esempi tratti sia dal settore pubblico sia da quello privato, al termine della quale è stata predisposta una "dichiarazione" adottata da Jacob Konstamm (Presidente del Comitato esecutivo della Conferenza internazionale) e dall'Autorità uruguaiana [v. doc. web n. 2375042].

Nel corso della sessione sono state inoltre adottate le risoluzioni sul futuro della *privacy* [v. doc. web n. 2375251] e sul *cloud computing* [doc. web n.2375241].

Sono state altresì deliberate le ammissioni di nuove autorità come componenti (Colombia, Costa Rica, Perù, Norvegia, Serbia, Tunisia, Sud Corea) e come osservatori (AFPDP-rete delle autorità francofone, OAS-Organizzazione degli Stati Americani) ed è stata accolta la proposta dell'Autorità polacca di tenere in Polonia la 35ª Conferenza internazionale (Varsavia 24-27 settembre 2013).

La Conferenza delle autorità europee (*Spring Conference* 2012)

La *Spring Conference* del 2012, tenutasi a Lussemburgo dal 3 al 4 maggio 2012, anch'essa focalizzata sulle proposte di riforma del quadro legislativo comunitario in materia di protezione di dati, ha adottato una risoluzione [doc. web n. 2375261] con la quale ha auspicato un sempre maggiore coinvolgimento delle autorità garanti nella discussione e nell'attuazione della proposta stessa, nonché un quadro più coerente di princìpi, con meno deroghe ed eccezioni per quanto concerne i trattamenti regolati dalla proposta di direttiva.

Durante la *Spring Conference* è stato deciso di porre termine all'attività del WPPJ (*Working Party on Police and Justice* -Relazione 2011 p. 199). Il prof. Francesco Pizzetti (Presidente dell'Autorità fino a giugno), che ha assicurato la presidenza nei quattro anni di vita del

gruppo, è stato calorosamente ringraziato per l'incisiva attività svolta, così come i funzionari del Garante. La Conferenza ha, quindi, accolto la relazione conclusiva dei lavori svolti dal WPPJ e dal suo Presidente.

Su proposta del comitato di accreditamento sono entrate a far parte della Conferenza le Autorità del Montenegro e della Bosnia-Herzegovina.

L'Autorità di protezione dei dati portoghese si è offerta di organizzare la prossima Conferenza di primavera a Lisbona.

21.3. LA COOPERAZIONE TRA AUTORITÀ NELL'UE: GRUPPO ART. 29

La cooperazione tra autorità garanti nell'UE è continuata nel 2012 in seno al Gruppo Art. 29 come da programma di lavoro adottato a febbraio 2012 (WP 190 [doc. web n. 2375271]).

Il Gruppo si è riunito in sessione plenaria 5 volte, per un totale di dieci giorni. Tutto il lavoro preparatorio è stato svolto come d'abitudine, nei sottogruppi tematici che hanno tenuto complessivamente oltre trenta riunioni, molte delle quali di due giorni.

Si segnala in particolare che dei 7 pareri adottati, 2 hanno riguardato il pacchetto di riforma (1/2012 e 8/2012) curati dal sottogruppo "*Future of Privacy*" e 4 l'applicazione dei princìpi di protezione dei dati nell'ambito delle nuove tecnologie e 1 sul livello di protezione dei dati personali nel Principato di Monaco. Oltre ai pareri formali, il Gruppo ha predisposto 3 documenti di lavoro (rispettivamente riguardo le *Binding corporate rules* e il progetto *epSOS* - v. Relazione annuale 2011 p. 198) ed inviato 19 lettere, in particolare a Google Inc., riguardo ai cambiamenti della *privacy policy* degli utenti e alla DG TAXUD della Commissione sul *Foreign Account Tax Compliance Act* (FATCA, v. *infra*).

Interpretazione di disposizioni "chiave" della Direttiva n. 95/46/CE: concetto di "finalità" e "trattamento compatibile"

Il Gruppo Art. 29, mantenendo il suo ruolo di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha continuato nel 2012 a contribuire alla corretta interpretazione ed applicazione di nozioni fondamentali della Direttiva base n. 95/46/CE e, mediatamente, al dibattito sulla revisione del *data protection legal framework*. Il lavoro del sottogruppo *Key provisions* si è concentrato sul concetto di "finalità" e "trattamento compatibile", ai fini dell'adozione, di un parere previsto nel 2013.

Il testo del parere viene costruito in modo da fornire una vera e propria guida per l'applicazione pratica del principio di finalità, nell'attuale quadro giuridico, anche attraverso raccomandazioni per il futuro. Si parte dall'analisi del *background* storico/normativo (dalla Convenzione n. 108/81 alla Direttiva n. 95/46/CE, alla proposta di regolamento generale della protezione dati) rispetto al principio di "finalità" ed alle sue declinazioni (comprese le raccomandazioni settoriali sviluppate dal Consiglio d'Europa (CoE) nel corso degli anni), si passa poi all'analisi delle disposizioni pertinenti della Direttiva n. 95/46/CE (artt. 6 e 13, considerando 28 e 29) corredata da esempi desunti dalle esperienze nazionali, per poi concludere con alcune osservazioni in tema di prospettive e sviluppi, alla luce delle recenti proposte di modifiche della normativa (ad es., revisione del *data protection framework*, proposte di riutilizzo dei dati del settore pubblico, ulteriore trattamento per scopi storici, statistici o scientifici; art. 13 della direttiva *e-privacy* sulle comunicazioni indesiderate, *open data*).

L'*opinion* dovrebbe ben evidenziare come il principio di finalità protegga gli interessati (fissando limiti sull'utilizzo dei loro dati), offrendo al tempo stesso un certo grado di flessibilità per i responsabili del trattamento. Il concetto di limitazione delle finalità viene costruito secondo due "blocchi principali": i dati personali devono essere raccolti per determinate, esplicite e legittime finalità e non essere successivamente trattati in modo compatibile con tali finalità. La compatibilità dell'ulteriore trattamento per uno scopo diverso, deve essere valutata caso per caso, ed a tal fine molto utili potranno risultare esempi basati sulla prassi delle autorità europee di protezione dei dati.

Questa analisi ha anche conseguenze per il futuro. Poiché l'art. 6(4) della proposta di regolamento sulla protezione dei dati restringe fortemente l'ambito di applicazione del principio della compatibilità, il Gruppo Art. 29 intende inserire nel parere specifiche proposte di modifica del testo.

Privacy e tecnologie

Un elemento-chiave sul quale il Gruppo Art. 29 si è concentrato nel 2012, in merito al rapporto fra protezione dati e tecnologie, ha riguardato la crescente perdita di controllo da parte dell'utente (ma anche del titolare, in taluni casi) sui propri dati. Che si tratti di tecnologie basate sul *cloud computing* o di applicazioni per telefonia mobile, o delle tecniche di profilazione basate sul monitoraggio della navigazione *online*, la cd. "autodeterminazione

informativa" -ovvero il potere dell'interessato di decidere in merito all'utilizzo dei suoi dati personali- è messa sempre più a rischio da modalità di trattamento non trasparenti e non rispettose dei princìpi fondamentali fissati nelle norme europee e nazionali in materia, soprattutto il diritto ad essere informati con chiarezza e il diritto ad esprimere un consenso pienamente valido prima di affidare i propri dati ad altri.

Parere sul *cloud computing*

Con il parere sul "*cloud computing*" (Parere n. 5/2012 - WP 196 [doc. web n. 2133003]), approvato il 1° luglio 2012, sono state fissate una serie di raccomandazioni per clienti e fornitori di servizi *cloud*, per garantire il rispetto dei princìpi di protezione dati, secondo i princìpi fissati dalla Direttiva n. 95/46/CE. Il parere, del quale l'Autorità italiana è stata co-redattrice, si concentra sulle garanzie di ordine contrattuale che dovrebbero essere rispettate sia da parte dei fornitori di servizi *cloud*, sia da coloro (pp.aa. o soggetti privati) che acquistano servizi in modalità *cloud*; evidenzia i rischi principali di queste tecnologie (perdita di controllo sui dati trasferiti nella "nuvola" e ridotta trasparenza delle operazioni di trattamento "delocalizzate"); analizza la problematica del trasferimento dei dati verso Paesi terzi; suggerisce il ricorso a forme di certificazione del fornitore *cloud* da parte di soggetti esterni ed indipendenti. Il parere contiene quindi un elenco dettagliato di misure tecnologiche di protezione per ovviare ai rischi sopra indicati, e si conclude con una serie di raccomandazioni sintetiche rivolte a fornitori e clienti su tutti gli aspetti affrontati, a partire dalla necessità per un cliente di servizi *cloud* di condurre preliminarmente una valutazione dei rischi per decidere se e come allocare dati personali nella "nuvola". Un allegato al parere illustra in sintesi le caratteristiche di funzionamento della tecnologia *cloud* ed i modelli di prestazione del servizio attualmente esistenti. Il parere evidenzia, inoltre, alcuni nodi tuttora irrisolti, *in primis* la circostanza per cui i principali fornitori di servizi *cloud* sono situati al di fuori dell'UE, ciò che rende più difficile il controllo del trattamento dei dati per le Autorità di controllo e per gli stessi utenti, ma anche per le stesse forze di polizia e giudiziarie, specialmente laddove le informazioni siano memorizzate in Paesi terzi ove non esista un livello "adeguato" di protezione dati.

Esenzione dal consenso per i *cookie*

I temi del consenso e della trasparenza sono al centro anche del parere adottato il 7 giugno 2012 (Parere n. 4/2012 - WP 194 [doc. web n. 2133013]) con cui sono state illustrate, in

particolare, le situazioni in cui si applica l'esenzione dall'obbligo generale di acquisizione del consenso per l'accesso o la registrazione di informazioni (in particolare i cd. "*cookie*" sul terminale dell'utente, ai sensi dell'art. 5(3) della Direttiva n. 2002/58/CE (direttiva "*e-privacy*") come modificata dalla Direttiva n. 2009/136/CE.

In base all'art. 5(3) della Direttiva n. 2002/58/CE, il previo consenso non è richiesto se il *cookie* serve al solo scopo di veicolare la trasmissione di una comunicazione sulla rete, oppure se "strettamente necessario" alla fornitura di un servizio della società dell'informazione richiesto espressamente dall'utente/contraente. Va sottolineato che l'art. 5(3) menziona il diritto a conoscere preventivamente ed autorizzare l'accesso o la registrazione di "informazioni" sul proprio terminale (si pensi, ad es., a programmi *spyware* o ad altre forme di intervento illecito sul terminale dell'utente/contraente). L'analisi dettagliata condotta nel parere evidenzia come, sostanzialmente, i *cookie* impiantati nel terminale dell'utente/contraente direttamente dal titolare del singolo sito web (cd. "*first-party cookies*") non necessitano del previo consenso se non sono utilizzati per altri scopi come *cookie* di sessione utilizzati per "riempire il carrello" in caso di acquisti *online*; quelli utilizzati per contenuti multimediali tipo *flash player* se non superano la durata della sessione, ed infine quelli di personalizzazione linguistica. Viceversa, per i *cookie* impiantati da "terze parti" (diverse dal titolare), in particolare per scopi di natura pubblicitaria, permane l'esigenza del consenso perché essi non soddisfano nessuno dei due requisiti sopra ricordati, come già segnalato dal Gruppo Art. 29 in precedenti pareri sul tema "pubblicità comportamentale" (*Behavioural Advertising* - v. Relazione 2011 p. 192). Anche i *cookie* utilizzati per fini di analisi degli accessi o delle visite al proprio sito (*analytics cookies*) non richiedono il previo consenso se perseguono esclusivamente scopi statistici e raccolgono informazioni in forma aggregata, a condizione che l'informativa fornita dal sito web sia chiara e adeguata e si offrano agli utenti modalità semplici per opporsi al loro impianto (*opt-out*, meccanismi di anonimizzazione). Il parere ricorda che, in caso di dubbio sull'applicabilità dell'esonero, è preferibile chiedere il consenso degli utenti/contraenti, al fine di garantire la liceità dei trattamenti svolti.

Mobile apps (applicazioni per telefonia mobile)

Nel 2012 il Gruppo ha lavorato alla predisposizione di un parere sulle *mobile apps* (applicazioni per telefonia mobile), in particolare esaminando gli obblighi e le raccomandazioni

da rivolgere ai diversi soggetti coinvolti nella creazione e distribuzione di tali applicazioni (sviluppatori, rivenditori/distributori, produttori dei sistemi operativi e degli apparecchi di telefonia mobile, soggetti terzi quali i fornitori di pubblicità o servizi di analisi). È stata in particolare evidenziata la mancanza di consapevolezza degli utenti sul trattamento dei loro dati, specie sensibili, da parte di soggetti terzi (si pensi al caso dei dati sanitari caricati con un'*app* sanitaria o alle informazioni bancarie che vengono comunicate ad un *app store*, o alle informazioni di localizzazione). Lo schema di parere evidenzia, quindi, da un lato le deficienze del sistema di sviluppo, produzione e distribuzione delle *app*, scarsa trasparenza per quanto riguarda le finalità dei trattamenti, l'assenza di un vero consenso da parte degli utenti finali; l'insufficienza delle misure di sicurezza; la tendenza alla "massimizzazione dei dati" e l'eccessiva elasticità degli scopi per i quali si procede a trattamenti ulteriori dei dati personali raccolti. Dall'altro canto, si richiamano i diversi soggetti coinvolti alle rispettive responsabilità. In primo luogo, gli sviluppatori di *app,* che devono ottenere il previo consenso degli interessati (specifico, informato, revocabile) e raccogliere solo i dati necessari per la funzionalità prescelta. Gli sviluppatori hanno un ruolo da svolgere anche nel promuovere buone prassi attraverso il "*rating*", cioè l'assegnazione di un punteggio di valutazione delle proprie *app*, sulla base dei meccanismi di *privacy* e sicurezza disponibili quali una *privacy policy* comprensibile e di facile accessibilità, nonché meccanismi a misura di utente per esercitare i diritti riconosciuti dalla direttiva e dal Codice. In tal modo gli interessati sarebbero sensibilizzati rispetto alla scelta delle *app*, che avverrebbe anche in base a quanto un'*app* sia "a misura di *privacy*". Ai distributori di *app* compete di facilitare il compito degli sviluppatori, indirizzando gli utenti verso le informazioni corrette, ed ai produttori di sistemi operativi e dispositivi "*smart*" quello di rendere tecnicamente possibile la realizzazione dei princìpi di trasparenza, correttezza, pertinenza e necessità nonché la raccolta di un consenso cd. "granulare", ossia un consenso adeguatamente modulato in relazione alle specifiche finalità del trattamento. Fondamentale è quest'ultimo requisito anche nei confronti dei soggetti terzi (pubblicitari, fornitori di servizi) che partecipino al sistema *app* a qualunque titolo: ad esempio, i soggetti operanti nel settore pubblicitario devono astenersi dall'invio di annunci pubblicitari estranei al contesto delle *app*, a meno di ottenere il previo consenso inequivocabile dell'utente; quindi non è consentito

inviare annunci modificando le impostazioni del *browser* o inserendo icone sul *desktop* dello *smartphone*. Tutti questi requisiti divengono ancora più pressanti per *app* rivolte (anche solo potenzialmente) ai minori per le quali vi sono obblighi più stringenti rispetto al consenso, all'informativa, ed alla scelta di modalità e linguaggi idonei a far comprendere ai soggetti minorenni la natura e gli scopi dei trattamenti previsti. Qui lo schema di parere fa appello alla creatività degli sviluppatori e distributori di *app*, che sono in grado di individuare gli approcci più idonei a tale scopo.

Parere sugli sviluppi nelle tecnologie biometriche

Attraverso il parere sugli sviluppi nelle tecnologie biometriche (Parere n. 3/2012 - WP 193 [doc. web n. 2375294]) è stato fornito un quadro aggiornato di linee-guida generali e di raccomandazioni sull'applicazione dei princìpi di protezione dei dati in ambito biometrico.

Il parere, rivolto alle autorità legislative europee e nazionali, all'industria dei sistemi biometrici e agli utenti di tali tecnologie, si sofferma sulle definizioni pertinenti del settore, sui princìpi fondamentali di protezione dei dati (finalità, proporzionalità, accuratezza, minimizzazione, sicurezza, criteri di legittimità del trattamento), sui nuovi sviluppi e tendenze in ambito biometrico e, anche attraverso specifici esempi, indica misure tecniche e organizzative per attenuare i rischi per la protezione dei dati e la vita privata dei cittadini europei.

Riconoscimento facciale

Con specifico riferimento al tema del riconoscimento facciale, un ulteriore approfondimento è stato condotto dal Gruppo Art. 29 (Parere n. 2/2012 - WP 192 [doc. web n. 2375284]) in relazione alle applicazioni *online* e di telefonia mobile. Il testo mette in luce i rischi di tali tecnologie, con particolare riguardo alla tipologia di dati trattati e alle finalità del trattamento e chiarisce che sono dati personali sia le immagini digitali, se contengono il volto visibile di una persona, sia i "modelli" (*templates*) ricavati dal trattamento delle immagini stesse. Il riconoscimento facciale può essere dunque effettuato solo nel rispetto dei princìpi fondamentali in materia di protezione dei dati, in particolare informando chiaramente gli utenti sui trattamenti previsti ed ottenendo il loro preventivo consenso in caso di "taggatura" delle immagini, sicché un utente non registrato o che non abbia dato il consenso non potrà essere "taggato" automaticamente in un *social network*. Per altro verso, sono possibili senza consenso alcune operazioni di trattamento fondate sull'interesse legittimo del titolare: ad es., un *social network* deve poter effettuare alcune operazioni

sull'immagine del volto per stabilire se una persona sia già "conosciuta" dal servizio ed abbia o meno acconsentito al "*tagging*" o ad ulteriori trattamenti. È indispensabile, infine, che siano adottate misure di sicurezza sia per la conservazione delle immagini che per il loro trasferimento in rete attraverso sistemi di cifratura.

I rapporti con Google

Va altresì segnalata una serie di iniziative che, a vari livelli, hanno riguardato i rapporti fra le autorità europee di protezione dati e Google Inc..

In primis, occorre menzionare la modifica apportata il 1° marzo 2012 da Google Inc. alla propria *privacy policy*, che prevede in via generalizzata la possibilità di incrociare e combinare dati relativi a più servizi offerti da Google. Il Gruppo Art. 29 ha deciso di valutare la conformità della nuova *privacy policy* con la normativa europea in materia di protezione dati, attraverso un'azione congiunta coordinata dall'Autorità francese per la protezione dei dati (CNIL). Google ha collaborato allo svolgimento di tali accertamenti rispondendo a due questionari inviati dalla CNIL rispettivamente il 19 marzo e il 22 maggio 2012, spiegando, fra l'altro, che molte delle prassi seguite in materia di *privacy* non si discostano da quelle di altre aziende statunitensi operanti su internet. Tuttavia, l'analisi delle risposte ai questionari ha evidenziato numerose problematiche con riguardo al mancato rispetto da parte della società americana di princìpi basilari della protezione dati. In primo luogo, gli accertamenti hanno dimostrato che Google non fornisce sufficienti informazioni agli utenti, in particolare rispetto alle finalità ed alle categorie di dati oggetto di trattamento. Ne consegue che l'utente non è in grado di stabilire quali categorie di dati siano trattate per il servizio di cui sta usufruendo, e per quali scopi tali dati siano trattati. In secondo luogo, gli accertamenti hanno confermato i rischi legati alla combinazione di dati tratti da servizi spesso molto diversi. La nuova *privacy policy* permette a Google di combinare sostanzialmente qualsiasi dato tratto da qualsiasi servizio per qualsivoglia finalità, ma in molti casi manca un'idonea base giuridica: talora manca il consenso inequivocabile dell'utente, oppure viene considerato erroneamente prevalente l'interesse legittimo di Google ad effettuare una raccolta massiva di informazioni, o non esiste alcun fondamento contrattuale per i trattamenti e gli incroci di dati effettuati. Resta da dimostrare, in molti casi, che i dati raccolti siano proporzionati agli scopi del trattamento:

Google non ha posto alcun limite ai possibili incroci di dati né ha fornito agli utenti strumenti che consentano loro di mantenere il controllo su tali operazioni di trattamento. Per tutti questi motivi, il 16 ottobre 2012 il Gruppo ha rivolto a Google in via ufficiale varie raccomandazioni per migliorare le informative, chiarire le modalità di incrocio dei dati e, più in generale, garantire l'osservanza delle norme e dei princìpi in materia di protezione dei dati con meccanismi semplificati di opposizione, raccolta del consenso espresso ai fini della combinazione di dati per determinate finalità, limitazione degli incroci di dati relativi ad utenti passivi. Il Gruppo ha concesso un periodo di quattro mesi a Google per le proprie valutazioni [doc. web nn. 2375141 e 2375151].

Bisogna ricordare in questa sede anche il contenzioso che oppone Google Inc. all'Autorità spagnola di protezione dati (APD), nel quale la Corte Suprema spagnola (*Audiencia Nacional*) ha formulato un rinvio pregiudiziale alla Corte di giustizia UE, al fine di stabilire se Google Inc. sia tenuta a rispondere alle richieste di cittadini spagnoli di cancellare i dati contenuti nelle stringhe di ricerca, e in che modo tale diritto all'oblio debba eventualmente essere esercitato. Secondo Google, che non riconosce l'applicabilità della normativa UE (e spagnola) così come sancita delle disposizioni di cui all'art. 4(1)c. della Direttiva n. 95/46/CE, la competenza esclusiva è delle autorità giudiziarie statunitensi. Il caso nasce da un ricorso presentato all'APD con riguardo alla pubblicazione di una notizia su un quotidiano, risalente a vari anni prima, che continuava ad apparire fra i risultati della ricerca effettuata digitando il nominativo della persona interessata. L'APD ha attribuito la responsabilità di agire per tutelare il diritto all'oblio a Google Inc. (tramite Google *Spain*) che invocando la propria natura di mero intermediario, ha negato la propria responsabilità per i contenuti raccolti in rete dal motore di ricerca. In una nota esplicativa dell'APD si evidenzia come la *Audiencia Nacional* sottolinei la necessità di un'interpretazione che prescinda dalla localizzazione dello strumento eventualmente utilizzato dal titolare *extra*-UE e, piuttosto, tenga conto dell'intera costellazione di elementi che formano il trattamento in oggetto, alla luce della natura di diritto fondamentale che ha assunto la protezione dei dati; secondo l'*Audiencia Nacional* dovrebbe prevalere il criterio del "*centro di gravità del conflitto*" tenendo conto di tutti gli interessi in gioco e delle norme implicate.

ICANN e registro *Whois*

Uno scambio di lettere fra il Gruppo Art. 29 e l'ICANN *(Internet Corporation for Assigned Names and Numbers*, con sede negli USA -ossia l'organismo di diritto privato- che assegna i nomi al dominio) ha permesso di evidenziare una serie di problematiche legate alla revisione di alcuni accordi ("*Registrar Accreditation Agreement, RAA*" e "*RAA Negotiations Summary Memo*") che disciplinano le modalità di registrazione e di accesso alle informazioni (dati identificativi di contatto per la gestione tecnica dei siti web) contenute nel registro denominato "*Whois*". Il Gruppo ha evidenziato le criticità relative alle forti pressioni di autorità giudiziarie e di polizia (USA e non solo) per accedere ai dati *Whois*, nonché alla possibile aggiunta, e verifica periodica, di informazioni ulteriori quali numero telefonico e indirizzo e-mail del registrante. Inoltre, il Gruppo ritiene sproporzionato l'allungamento dei tempi di conservazione dei dati contenuti in *Whois* (24 mesi) dopo la cessazione del contratto relativo ad un dominio web. Da parte sua, ICANN ha risposto che queste tematiche sono in corso di trattazione da parte della *Government Advisory Committee (GAC)* dell'ICANN stesso, di cui fa parte anche un rappresentate della Commissione europea, e che pertanto occorre assicurare il coordinamento con il rappresentante della Commissione al fine di segnalare in modo appropriato le criticità relative alla revisione del *RAA*. Inoltre, ICANN ha dichiarato che sarà aggiornato anche il meccanismo relativo ai casi in cui il *RAA* confligga con la normativa *privacy* (anche nazionale) del registrante, tramite la previsione di specifiche deroghe.

La nuova attività congiunta sui temi *Borders, Travel* e *Law Enforcement*

Nel 2012, il Gruppo Art. 29 ha dato il via all'attività del sottogruppo *Borders, Travel and Law Enforcement subgroup* (BTLE), sulle tematiche connesse al trattamento di dati nel settore di polizia e giustizia (*ex* III Pilastro), in seguito alla soppressione del WPPJ nel corso della *Spring Conference* 2012 e in ragione dell'unificazione dei pilastri dell'Unione dopo l'entrata in vigore del Trattato di Lisbona (v. *infra Spring Conference* 2012).

In tale quadro il Gruppo Art. 29 ha seguito l'andamento della discussione al Parlamento europeo della proposta presentata dalla Commissione per l'introduzione di un sistema europeo di raccolta e trattamento dei dati dei passeggeri aerei (EU PNR - *Passenger Name Record*) ed ha espresso, insieme al Consiglio, Commissione e Parlamento, forti preoccupazioni in relazione al possibile accordo PNR con il Canada.

Si segnalano inoltre le lettere inviate dal Gruppo alla Commissaria Malmström il 12 giugno 2012 [doc. web nn. 2375181 e 2377470], per esprimere le proprie preoccupazioni in merito ai profili di protezione dati delle proposte della Commissione contenute nella comunicazione in materia di *smart borders* ("frontiere intelligenti", COM(2011) del 25 ottobre 2011) ed alla proposta di regolamento che istituisce un sistema europeo di sorveglianza delle frontiere (Eurosur: frontiere sud dell'Unione con i Paesi del bacino mediterraneo COM(2011) 873 del 12 dicembre 2011). Entrambi i sistemi hanno come finalità principale la lotta all'immigrazione clandestina ed il miglioramento del controllo delle frontiere dell'UE, anche con dispositivi elettronici.

Quanto, poi, agli specifici argomenti di *law enforcement* si menziona l'accordo del 28 giugno 2010 tra l'Unione europea e gli Stati Uniti sul trattamento e il trasferimento di dati di messaggistica finanziaria, per il controllo delle transazioni finanziarie dei terroristi *(Terrorist Finance Tracking Program).* La seconda revisione congiunta delle modalità di funzionamento dell'accordo si è svolta il 29 e 30 ottobre 2012 con la presenza, per le autorità di protezione dati, di rappresentanti delle Autorità dei Paesi Bassi e del Belgio. Gli Stati Uniti hanno rappresentato in quale modo le varie disposizioni dell'accordo siano rispettate. Non sono stati forniti ulteriori dettagli sui risultati della verifica congiunta, né sulle informazioni ricevute dagli Stati Uniti. Tuttavia, il delegato della DPA dei Paesi Bassi ha espresso le proprie perplessità sulle modalità di funzionamento dell'accordo: il *focus* negli USA è spostato "dai dati alle persone" e ciò desta non poche preoccupazioni -condivise dal Gruppo- in termini di controllo e profilazione degli individui.

In relazione poi, all'accesso alle cd. "informazioni classificate", è stato fatto circolare tra le delegazioni del Gruppo Art. 29 un questionario, al quale il Garante ha risposto illustrando, in particolare, gli obblighi di segretezza gravanti sul personale addetto all'Ufficio del Garante e sui suoi consulenti (v. art. 156, comma 8 del Codice).

Protezione dei dati in ambito finanziario

Nel 2012 il Gruppo Art. 29 ha continuato ad occuparsi del trattamento dei dati in ambito finanziario, con particolare riferimento all'attuazione della legislazione statunitense per il contrasto delle frodi fiscali (cd. "*off shore Foreign Account Tax Compliance Act",* FATCA); all'attuazione degli accordi di cooperazione internazionale "*Public Companies Accounting*

Oversight Bodies" (PCAOB) stipulati tra Stati Uniti e Stati membri dell'Unione europea; alla revisione della legislazione in materia di contrasto alle attività di riciclaggio e finanziamento del terrorismo.

Con riferimento alla legislazione statunitense FATCA -che introduce l'obbligo di rilevare specifici dati dei clienti cittadini statunitensi da parte di istituti finanziari ed assicurativi insediati nell'Unione europea, e di trasferire tali dati all'amministrazione fiscale degli Stati Uniti, per contrastare l'evasione fiscale da parte di "*US persons*"- è stato dato particolare rilievo al problema generale della sua applicabilità *extra*-territoriale nei Paesi membri dell'Unione europea.

La legittimità del criterio previsto per l'applicazione delle disposizioni in parola (titolarità di conti o polizze assicurative da parte di "*US persons*") non è risultata chiara, anche in quanto la legislazione è stata adottata "in via unilaterale", al di fuori dei *fora* internazionali (OCSE), e sembrerebbe non in linea con i vigenti accordi internazionali per la prevenzione della doppia imposizione fiscale.

Oltre alla mancanza di un'idonea base giuridica per il trattamento dei dati personali da parte dei titolari nell'Unione europea, il Gruppo ha considerato le criticità derivanti dall'applicazione di FATCA anche alle società di assicurazione.

Circa la sopravvenuta conclusione, da parte del Dipartimento del Tesoro degli Stati Uniti di un accordo (al quale aderiscono Italia, Spagna, Germania, Francia, Regno Unito), preliminare alla conclusione di accordi bilaterali ed aperto alla successiva adesione di altri Stati membri, è stata sottolineata la necessità di definire con precisione le misure di protezione dei dati personali, i diritti degli interessati, l'ambito dei soggetti obbligati, esentando le operazioni a basso rischio (come quelle svolte dalle società assicurative), ed evidenziata altresì, l'opportunità di assicurare la reciprocità degli obblighi di cooperazione tra Stati membri dell'Unione europea e Stati Uniti.

Il Gruppo ha, quindi, segnalato alla Commissione europea (lettera 21 giugno 2012 [doc. web n. 2375072]) come possibile, benché più problematica, base giuridica per il trattamento dei dati personali anche il contratto/*agreement* tra operatori finanziari e amministrazione tributaria USA. In particolare, rispetto al precedente "approccio unilaterale" statunitense è

stato considerato preferibile un sistema basato sul trasferimento dall'autorità fiscale nazionale competente all'omologa autorità statunitense dei soli dati personali rilevanti, sulla base di accordi bilaterali tra Stati Uniti e Stato membro dell'Unione europea (cd. "*model I agreement*"). Maggiori criticità sono state invece ravvisate nell'opzione che prevede il trasferimento diretto dei dati dagli operatori finanziari al Dipartimento del Tesoro degli Stati Uniti (cd. "*model II agreement*"). Il Gruppo si è comunque riservato la possibilità di esaminare tali accordi in seguito.

Quanto agli accordi di cooperazione internazionale PCAOB stipulati tra Stati Uniti e Stati membri dell'Unione europea, nel corso della plenaria di dicembre 2012 il Gruppo ha raccomandato alla Direzione Generale mercato interno della Commissione europea (v. lettera del 13 dicembre 2012 [doc. web n. 2375161]) il ricorso da parte delle competenti autorità degli Stati membri ad un "protocollo *standard*" (*agreement for the exchange of information*) predisposto dalla Commissione europea, accompagnato da un protocollo addizionale contenente misure idonee ad assicurare la protezione dei dati personali, aggiuntive rispetto a quelle prescritte nel precedente parere del Gruppo Art. 29 (parere 10/2007 - WP 143). È stato inoltre predisposto un questionario, successivamente trasmesso dalla Commissione europea alle autorità nazionali competenti, per ottenere informazioni in merito allo *status* degli accordi (*Memorandum of Understanding*, cd. "MoU") eventualmente stipulati o in corso di elaborazione da parte delle autorità di controllo europee (in Italia, la Consob) con il PCAOB, anche al fine di valutare la conformità di tali accordi alle misure proposte nel precedente parere del Gruppo Art. 29.

Trasferimento dati all'estero

Nel 2012 sono stati oggetto di particolare attenzione i trasferimenti effettuati dai gruppi multinazionali d'impresa (mediante il perfezionamento di norme vincolanti d'impresa cd. "*Binding corporate rules for controller*") e quelli effettuati nell'ambito di forme di esternalizzazione delle attività di trattamento dei dati (v. le clausole contrattuali tipo 87/2010/UE, da titolare a responsabile, approvate dalla Commissione europea).

In merito, è stata condivisa l'esigenza manifestata dal mondo dell'impresa di disporre di un sistema semplificato per i flussi transfrontalieri di dati gestiti da società multinazionali di servizi, in grado di ricomprendere anche il caso (non contemplato dalle clausole contrattuali

tipo 87/2010/UE), in cui il responsabile sia stabilito in uno Stato membro. A tal fine è stato elaborato un nuovo modello di norme vincolanti d'impresa definito *Bcr for processor*.

Lo strumento è concepito su un doppio livello: il cliente (titolare) sottoscrive un contratto generale di servizi (*Service Level Agreement* - SLA) con la società multinazionale (responsabile); il contratto impegna le parti al rispetto di una serie di clausole tra le quali sono ricomprese le *Bcr for processor* (allegate allo SLA). Tramite le *Bcr for processor*, la società multinazionale ha la possibilità di "sub-appaltare" le attività di trattamento (o alcune fasi di esso) alle proprie consociate o affiliate anche stabilite in Paesi terzi, senza necessità di ulteriori formalità (quali ad es., autorizzazioni *ad hoc*, *standard contractual clauses*).

Lo schema di *Bcr for processor* ricalca quello delle *Bcr for controller* nei suoi princìpi fondamentali: efficacia vincolante delle *Bcr*, clausola del terzo beneficiario a favore dell'interessato, clausola di responsabilità con attrazione della giurisdizione in UE, rispetto dei princìpi della Direttiva n. 95/46/CE, impegno per il gruppo multinazionale di impresa a dotarsi di un sistema di *training*, a disporre di una struttura specializzata nella gestione delle segnalazioni degli interessati e a svolgere *audit* periodici sul rispetto dei princìpi di protezione dati da parte delle proprie affiliate. Il testo è stato adottato nel giugno 2012 (*Working Document* n. 02/2012 - WP 195 del 6 giugno 2012 [doc. web n. 2375532]).

Sempre in tema di trasferimento di dati all'estero, è stato adottato un parere che ritiene adeguato il livello di protezione dei dati personali nel Principato di Monaco (Parere 7/2012 - WP 198 [doc. web n. 2133808]) dopo aver attentamente valutato, in collaborazione con l'autorità locale (*Commission de Contrôle des Informations Nominatives* - CCIN) i criteri e i princìpi della normativa monegasca rispetto all'applicazione degli artt. 25 e 26 della direttiva europea.

Il Gruppo, con lettera del 3 marzo 2012 ha inoltre sollecitato la Commissione ad adottare le decisioni di esecuzione sull'adeguata protezione dei dati personali della Repubblica orientale dell'Uruguay e della Nuova Zelanda, rispettivamente sulla base dei pareri favorevoli del 12 ottobre 2010 (WP 177) e 4 aprile 2011 (WP 182), poi adottate il 21 agosto e il 19 dicembre 2012.

21.4. LA COOPERAZIONE DELLE AUTORITÀ NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Come riferito sopra, nel 2012 il Gruppo di lavoro Polizia e Giustizia (*Working Party on Police and Justice* - WPPJ) ha terminato i suoi lavori in seguito alla decisione presa dalla Conferenza europea delle autorità garanti svoltasi a Lussemburgo (v. *supra*). Le sue funzioni sono assorbite nelle competenze del Gruppo Art. 29, in particolare attraverso il sottogruppo BTLE, mentre sarà la Conferenza stessa, laddove necessario, a definire le modalità di intervento delle autorità europee su temi di più ampia rilevanza.

Si segnala inoltre l'entrata in vigore del VIS (Sistema informativo visti) che comporta una nuova attività di supervisione e controllo sulla legittimità dei trattamenti di dati da parte del Garante sia a livello nazionale, sia a livello europeo, attraverso il Gruppo di supervisione formato dalle autorità europee e dal Garante europeo, quale Autorità di controllo delle attività svolte da istituzioni ed organismi dell'Unione.

Si è riferito sopra anche della proposta di direttiva riguardo i trattamenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, che dovrebbe sostituire la Decisione quadro n. 2008/977, adottata prima dell'entrata in vigore del Trattato di Lisbona e che riguardava soltanto i princìpi necessari per consentire gli scambi di informazioni.

È comunque proseguita l'attività di supervisione e controllo svolta nelle Autorità comuni e nei Gruppi di supervisione già istituiti e menzionati nelle precedenti Relazioni.

Europol: l'attività dell'Autorità di controllo comune [Acc] e del comitato ricorsi

Nella riunione del 14 marzo 2012 è stato adottato il secondo rapporto d'ispezione sul trattamento da parte di Europol delle richieste di dati relativi a transazioni finanziarie europee, provenienti dal Tesoro americano in base all'Accordo UE-USA del 28 giugno 2010 per le esigenze del programma Tftp. Poiché gli atti relativi allo stesso accordo sono classificati come segreti, l'Acc ha deciso per ragioni di trasparenza di redigere la cd. "parte pubblica del rapporto" presentata con un breve comunicato stampa il 21 marzo 2012 [doc. web nn. 2375032 e 2375320]).

Per quanto riguarda il trattamento dati effettuato dalla Acc Europol (con riferimento agli archivi di analisi, al sistema di indice, al sistema di trasmissione dei dati), l'ispezione annuale presso la sede di Europol a L'Aja è stata svolta anche con la partecipazione di un esperto

tecnico del Garante. Alcune criticità riscontrate riguardano il sistema di trasmissione dati SIENA (che viene proposto come sistema generale di trasmissione per le comunicazioni tra Stati membri e per il quale Europol agisce come *service provider*) che necessiterebbe di una specifica base giuridica per definire adeguatamente ruoli, compiti e regole di accesso ai dati da parte dell'organizzazione. Il rapporto finale, adottato dall'Acc, contiene una serie di raccomandazioni in tal senso.

A completamento delle informazioni raccolte attraverso le ispezioni cd. "centrali" presso l'Europol, considerato il ruolo svolto dagli Stati attraverso le informazioni che inviano per l'analisi o per il sistema indice, l'Acc ha deliberato di verificare le condizioni di funzionamento degli uffici nazionali incaricati di scambiare informazioni con Europol. La verifica deve essere svolta in modo coordinato con una metodologia uniforme, predisposta dal segretariato ed approvata dall'Acc. Entro la prima metà del 2013 verrà pubblicato un rapporto con le risultanze delle verifiche e le raccomandazioni ritenute necessarie.

Nella riunione di dicembre 2012, l'Acc ha definito le tipologie di trattamenti che saranno oggetto dell'ispezione annuale, in programma nel marzo 2013; ha rinnovato il mandato al responsabile del *team* di ispezioni ed ai componenti (di cui fa parte un esperto tecnico del Garante) e deciso di includere nell'ordinaria ispezione annuale gli aspetti relativi al trattamento dati Tftp.

L'Acc ha, infine, adottato 2 pareri [doc. web nn. 2375221 e 2381001] sul livello di protezione dei dati in Serbia ed in Liechtenstein e un parere sull'accesso di Europol ad Eurodac [doc. web n. 2375211]; inoltre ha discusso aspetti relativi allo sviluppo del sistema di messaggistica SIENA ed adottato in principio il rapporto di attività relativo agli anni 2008-2012.

Il Comitato ricorsi non ha avuto riunioni nel 2012 e ciò perché la nuova risposta *standard* alle richieste di accesso, in caso di non esistenza di dati presso l'organizzazione, in linea con quanto suggerito più volte dall'Acc, sembrerebbe fornire elementi più chiari, sicché gli interessati non hanno presentato ricorsi all'Acc.

Nel 2012 è proseguita la valutazione delle risposte pervenute al segretariato sull'attività di verifica svolta a livello nazionale dalle autorità di protezione dati, relativamente alla legittimità delle segnalazioni inserite nel Sistema Informativo Schengen (SIS), per quanto

Il Sistema Informativo Schengen: l'attività dell'Autorità di controllo comune [Acc] Schengen

necessario a fini del mandato di arresto europeo. L'Acc, in vista della discussione della bozza del rapporto conclusivo, ha chiesto al segretariato di prendere contatti con l'Acc Eurojust per eventuali valutazioni e contributi.

Quanto alle segnalazioni a fini di non ammissione, ai sensi dell'art. 96 della Convenzione Schengen, l'Acc ha deciso di segnalare alla Commissione europea il conflitto tra le norme della Convenzione medesima, che richiedono una attenta e documentata decisione, caso per caso, sull'inserimento della segnalazione nel SIS -oltre che negli archivi nazionali- ed il divieto di ingresso regolato dalla direttiva "rimpatri" (Direttiva n. 2008/115/CE) che introduce invece un automatismo nell'inserimento delle segnalazioni [doc. web n. 2375381].

L'Acc ha anche adottato pareri in merito alla proposta di introdurre una funzione *SEarCH* nel SIS, ritenuta non necessaria in quanto già sviluppata in altri gruppi di lavoro ed alla migrazione dall'attuale SIS 1+ al SIS II.

L'entrata in funzione del SIS II, le cui basi giuridiche sono state adottate fin dal 2006, in programma per la primavera del 2013, comporterà anche la decadenza dell'Acc essendo prevista una diversa forma di supervisione comune, simile a quella istituita per altri sistemi di informazioni europei come Eurodac e Vis. Poiché la transizione potrebbe avere una durata maggiore del preventivato, il parere dell'Acc richiama l'attenzione della Commissione -che gestirà il nuovo sistema con l'Agenzia- sulla necessità di evitare vuoti nella supervisione e controllo dei trattamenti durante la fase transitoria.

Il Sistema informativo doganale [Sid]: Cis Supervision Coordination Group e attività dell'Acc

L'attività dell'Acc Dogane è stata nel 2012 limitata ai temi correnti mentre si sta sviluppando quello del Cis *"Supervision Coordination Group"* (Gruppo di coordinamento della supervisione del Sid). Al riguardo la Commissione ha comunicato che si sta predisponendo una modifica degli strumenti normativi esistenti, che è stato redatto un primo rapporto sull'impatto dell'intervento, che dovrà, una volta approvato dal *board* della Commissione, essere presentato alla consultazione interservizi, entro il luglio del 2013. La proposta dovrebbe contenere norme sulla supervisione ben coordinate e senza ambiguità.

L'Acc Dogane aveva al riguardo stimolato l'azione della Commissione al fine di valutare la necessità del mantenimento di una Autorità comune di supervisione e controllo sulla

legittimità dei trattamenti dei dati nel Sid, data l'esiguità dei dati scambiati nel sistema e la netta preferenza delle amministrazioni doganali per i canali bilaterali di cooperazione.

Gruppo di supervisione Vis (Sistema informativo visti)

Il Gruppo di coordinamento e supervisione Vis è stato istituito dall'art. 43 del Regolamento (CE) n. 767/2008 per monitorare la liceità del trattamento dei dati personali sia da parte delle autorità di gestione nazionali, sia da parte dell'Autorità di gestione del Vis centrale, anche attraverso periodici *audit* di controllo. Il Gruppo ha tenuto la sua prima riunione, provvisoriamente diretta dal Garante europeo per la protezione dei dati P. Hustinx, il 21 novembre 2012.

Nel corso della riunione si è approvata una prima bozza di regolamento preparata dal segretariato in via provvisoria con riserva delle modifiche richieste da alcune delegazioni. Si è anche deciso di posporre la nomina del presidente alla prossima riunione e si è accolta la richiesta presentata dall'Irlanda di poter prender parte alla riunione in qualità di osservatore. Per la successiva riunione -prevista nella primavera del 2013- sarà autorizzata anche la presenza del rappresentante del Regno Unito (che, con l'Irlanda non è parte della cooperazione Schengen). Rappresentanti della Commissione hanno informato sullo sviluppo graduale del sistema, per regioni del mondo predefinite in base a decisioni della Commissione, che dovrebbe essere completato per la seconda metà del 2013, nonché sul trasferimento di competenze per la gestione operativa del VIS centrale (C-VIS) dalla Commissione all'Agenzia appositamente creata (*Large scale IT Agency*).

Il Gruppo Vis ha poi discusso con l'EDPS (Garante europeo per la protezione dei dati) dei risultati dell'*audit* eseguito sul sistema e sul seguito dato dalla Commissione alle raccomandazioni formulate. Sono state presentate esperienze di visite e verifiche svolte in alcuni consolati da parte delle Autorità di protezione dei dati della Svizzera e della Francia (basate anche sulla verifica degli obblighi previsti dalla Convenzione Schengen).

Si è inoltre discussa la bozza del programma di attività per il biennio 2013-2014 e si è convenuto di prevedere, nel rispetto del regolamento Vis (Regolamento CE n. 767/2008 del 9 luglio 2008), coordinate attività di verifica sia sul sistema centrale sia sulle parti nazionali del Vis (inclusa la verifica del modo in cui le forze dell'ordine hanno accesso ai dati secondo quanto previsto dalla Decisione n. 633 del 2008), garantendo però che le relative decisioni

siano prese nel rispetto delle priorità nazionali di ciascuna autorità. Questo anche con riferimento alla frequenza e alle modalità di riunione del Gruppo, che dovrà coordinarsi con il Gruppo Eurodac e con le altre forme di supervisione comune, per evitare sovrapposizioni di date e di concomitanti richieste di svolgere accertamenti nazionali.

Gruppo di supervisione Eurodac

Nel maggio 2012 il Gruppo di supervisione Eurodac, istituito per verificare la legittimità del trattamento dei dati nel sistema Eurodac (contenente le impronte digitali dei richiedenti asilo nei Paesi UE) ha conferito un secondo mandato di Presidente e Vicepresidente a P. Hustinx ed E.Wallin.

Il Gruppo ha discusso, tra l'altro, il progetto della Commissione relativo al regolamento Eurodac, che consentirebbe l'accesso ai dati contenuti in Eurodac alla forze di polizia. In merito, anche i rappresentanti dell'UNHCR (Alto Commissariato delle Nazioni Unite per i rifugiati), presenti alla riunione di maggio, hanno espresso le loro preoccupazioni rispetto alla proposta, che consente ricerche, a fini di polizia, anche a partire da frammenti di impronta ritrovati sulla scena del crimine. L'accesso ai dati sarà consentito a polizia, inquirenti e ad Europol solo qualora dall'interrogazione delle esistenti banche dati di polizia non emergano riscontri. Tale limitazione è stata peraltro ritenuta non sufficiente. La proposta, presentata il 30 maggio 2012 (COM(2012) 254 definitivo) è stata discussa in incontri trilaterali anche con il Parlamento ed il Consiglio.

Il Gruppo ha poi adottato il rapporto di attività per gli anni 2010 e 2011 [doc. web n. 2375052].

Sulla scorta di lavori pilota svolti da alcune delegazioni, il Gruppo ha messo a punto un piano di ispezione standardizzato, da utilizzare a livello nazionale per l'attività di supervisione e controllo attribuita dal regolamento Eurodac.

Nel 2012, il Gruppo di supervisione Eurodac ha anche svolto verifiche sul trattamento delle impronte digitali illeggibili e sulle eventuali conseguenze sulla procedura di asilo. Infatti, dal momento che il regolamento Eurodac prevede l'inserimento delle impronte nel sistema per verificare se corrispondono ad altre già contenute, il fatto che la persona non abbia impronte digitali "leggibili" dalle macchine usate (*live scan)* non può influire sull'accesso alla procedura di asilo poiché questo comporterebbe l'introduzione di un

ulteriore requisito -la presenza di impronte digitali leggibili- non previsto dal Regolamento "Dublino" di cui il Sistema Eurodac è servente. Il Gruppo ha inoltre cominciato una riflessione sul programma di lavoro per il biennio 2013-2014, nel corso della quale sono emerse preoccupazioni sul crescente carico di lavoro e quindi sull'opportunità di ridurre e rendere sinergiche le richieste di attività da svolgere a livello nazionale, come evidenziato anche in riferimento ai lavori del Gruppo VIS.

In ogni caso il programma di lavoro potrà essere definito solo una volta adottata la nuova base legale, dovendosi fissare tempi e forme per l'esercizio di una efficace supervisione a livello centrale sulla banca dati ed a livello nazionale sull'inserimento dei dati e l'uso del sistema da parte degli Stati.

21.5. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Il "Gruppo di Berlino" - *International Working Group on Data Protection in Telecommunication* IWGDPT

La 51ª e 52ª riunione dell'*International Working Group on Data Protection in Telecommunications* (Gruppo di Berlino) si sono svolte il 23 e 24 aprile 2012 a Sopot (Polonia) e 10 e 11 settembre a Berlino.

Nel corso della prima riunione il Gruppo ha adottato un documento di lavoro (*Sopot Memorandum*) [doc. web n. 2375062], che contiene raccomandazioni generali volte a ridurre i rischi associati all'utilizzo del *cloud* ed a promuoverne uno sviluppo responsabile. In particolare il Gruppo raccomanda che: il *cloud computing* sia accompagnato da un livello di tutela di dati personali adeguato e non inferiore a quanto previsto negli altri ambiti; i titolari del trattamento valutino preliminarmente l'impatto di tali tecnologie sui diritti delle persone; i fornitori di servizi di *cloud* sviluppino pratiche in grado di garantire trasparenza, sicurezza e fiducia, in particolare fornendo informazioni su possibili violazioni dei dati (*data breach)* e favorendo la portabilità e il controllo dei dati da parte degli utenti; siano incentivate la ricerca, la certificazione da parte di soggetti terzi, la standardizzazione, e le tecniche di *privacy by design*; i legislatori valutino l'adeguatezza del quadro normativo esistente riguardo al trasferimento dei dati; le autorità di protezione dei dati continuino a fornire le necessarie informazioni ai titolari del trattamento, ai fornitori di *cloud* e ai legislatori sulla protezione dei dati in tale ambito.

Il documento approvato contiene altresì diverse indicazioni concernenti le *best practices,* che dovrebbero essere adottate dai titolari del trattamento e dai fornitori di servizi di *cloud*.

Nel 2012 il Gruppo si è occupato anche del diritto all'oblio (*right to be forgotten*) in internet, affrontato da due prospettive. La prima riguarda il "diritto a non essere trovato", attraverso strumenti tecnici che consentano di limitare la reperibilità sul web di informazioni relative all'interessato. La seconda, di carattere prettamente giuridico, riguarda il "diritto a essere dimenticato", ossia l'insieme delle condizioni e dei contesti pubblici (ad es., diffusione attraverso mezzi di informazione, casi giudiziari) e privati (ad es., ambienti di lavoro, contesti sanitari) in cui l'interessato può legittimamente chiedere a un titolare di non trattare i propri dati personali.

Il Gruppo ha deciso di affrontare i due aspetti separatamente e di concentrarsi in prima battuta su un documento di lavoro, di cui l'Autorità è *rapporteur*, relativo agli strumenti tecnici che consentono all'utente -pur nel rispetto della libertà di espressione- di esercitare il proprio diritto a non essere rintracciato nella "rete", in particolare attraverso l'uso del protocollo *robots.txt* da parte dei gestori dei siti web, che permette di limitare l'indicizzazione -operata dai motori di ricerca- delle informazioni presenti in internet.

Il Gruppo si è occupato inoltre del tema del web *tracking*, ossia delle tecnologie per il tracciamento, a fini di pubblicità comportamentale, delle attività degli utenti svolte sui siti internet. La questione, oggetto di un parere in via di elaborazione, afferisce al sempre più frequente ricorso da parte degli utenti a servizi web di calendario e gestione di rubriche. Tali servizi, in passato resi da applicazioni che trattavano dati memorizzati sui terminali, oggi, per via della maggiore disponibilità di banda, memoria e potenza di calcolo disponibili in rete, vengono per lo più realizzati in modalità *cloud*, consentendo agli utenti una maggiore integrazione con altre applicazioni di natura gestionale o semplicemente di socializzazione.

Tra i maggiori rischi in questo campo per la protezione dei dati si evidenziano il potenziale trasferimento di dati di traffico al fornitore dell'applicazione e il ricorso a tecnologie di trattamento digitale delle immagini in grado di riconoscere volti e più in generale di ricostruire il contesto di riferimento dell'interessato (e segnatamente abitazione, luogo di lavoro, amicizie). Nelle proposte formulate si sottolinea l'esigenza di distinguere la fase di

raccolta dei dati (*collecting*) dal loro successivo uso (*tracking*), per regolare il trattamento in maniera più flessibile. Attenzione è stata anche prestata all'opportunità di richiedere "*test* di necessità e proporzionalità" da realizzare prima del lancio commerciale di una nuova applicazione, in modo da prevedere la possibilità di alternative "*privacy friendly*", rispetto ad ogni specifico trattamento.

Nel corso delle riunioni è stato anche affrontato il tema del trattamento dei dati nell'ambito di Google *analytics*, il servizio che consente di monitorare le attività svolte sul proprio sito web dagli utenti (cd. "*audience measurement*"). Sono stati in particolare considerati i profili critici relativi alla mancanza di una idonea informativa e all'assenza di procedure tecniche per l'anonimizzazione degli indirizzi *Ip* raccolti dai titolari e trasferiti al motore di ricerca.

Data retention-expert Group

Nel 2012 il Gruppo di lavoro si è riunito tre volte per continuare ad esaminare aspetti legati all'interpretazione di alcuni termini della Direttiva n. 2006/24/CE (cd. "direttiva *data retention*") nonché alla possibile revisione della medesima. Il Gruppo infatti assiste la Commissione nel verificare l'applicazione della suddetta Direttiva ed è composto da rappresentanti provenienti dall'industria TLC, dalle *Law enforcement agencies* degli Stati membri, nonché dai rappresentanti delle Autorità di protezione dati degli Stati membri e dall'EDPS.

La Commissione, sulla base dei lavori del Gruppo dello scorso anno, ha individuato una forte disomogeneità di applicazione della normativa negli Stati membri, dando mandato al Gruppo di redigere le linee-guida volte all'armonizzazione, che verranno verosimilmente pubblicate nei primi mesi del 2013. La Commissione ha anche chiesto indicazioni alle varie parti per poter sviluppare un progetto che da un lato definisca meglio la composizione del gruppo, mantenendo la tripartizione -dimostratasi utile-Governi/*Law Enforcement Authorities agencies - LEAs* (che include Europol), industria ed autorità di protezione dei dati, e dall'altro precisi mandato e modalità di azione del Gruppo, anche in vista della nuova proposta di direttiva che la Commissione potrebbe presentare nel 2013. Al riguardo la Commissaria Malmström, partecipando alla sessione plenaria del Parlamento europeo per rispondere ad alcune interrogazioni sul tema, nel confermare che i tempi di revisione della direttiva saranno

definiti in relazione all'andamento della discussione sul pacchetto generale di riforma della protezione dati, ha ribadito che nel nuovo testo sarà necessario tenere conto di diversi aspetti. In particolare, le aree della direttiva, *data retention* che devono essere migliorate -nella conferma della necessità di tale strumento- sono le seguenti: tempi di conservazione ridotti ed armonizzati; indicazione chiara degli scopi e dei tipi di dati che devono essere conservati; regole minime *standard* per l'accesso e l'uso dei dati; garanzie di protezione dati più forti e un approccio coerente sul tema del rimborso dei costi per gli operatori.

Consiglio d'Europa

L'Autorità ha continuato a partecipare ai lavori del Comitato consultivo (T-PD) della Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

L'attività del T-PD nel 2012, in gran parte dedicata alla modernizzazione della Convenzione n. 108, ha portato all'adozione, nella 29ª plenaria del Comitato, di un documento finale con il quale il T-PD, prendendo atto delle sfide tecnologiche e della globalizzazione emerse in maniera dirompente negli ultimi decenni, ribadisce la natura trasversale della Convenzione (che si riferisce ai trattamenti di dati sia in ambito pubblico sia in ambito privato), la sua vocazione universale (in quanto unico strumento vincolante a livello internazionale ed aperto alla ratifica anche di Stati che non sono membri del Consiglio d'Europa) ed il suo carattere "neutro" a livello tecnologico (si tratta infatti di princìpi generali che si applicano ai diversi settori indipendentemente dalla tecnologia utilizzata, in modo da evitare una rapida obsolescenza del testo) [(doc. web n. 2375191]).

Le modifiche proposte dal T-PD, per assicurare un quadro di princìpi coerenti con il progetto di revisione degli strumenti di protezione dei dati in discussione a livello UE, innovano tuttavia l'impianto definitorio della Convenzione, i criteri di legittimità del trattamento, la disciplina dei dati sensibili -comprensiva anche dei dati biometrici e genetici e le misure di sicurezza- con la previsione di un sistema di notifica in caso di *data breach.* Introducono inoltre doveri di trasparenza per il titolare del trattamento nonché la cd. "*accountability*" ed ampliano i diritti dell'interessato. Includono princìpi sui flussi transfrontalieri di dati e sulle autorità di controllo (attualmente previsti nel protocollo addizionale alla Convenzione), rafforzandone i poteri e l'indipendenza. Accrescono infine il

ruolo del Comitato della Convenzione specie con riferimento all'adesione di nuovi Stati ed all'attuazione dei suoi princìpi.

Alla fine del 2012, terminata la propria attività "tecnica", il T-PD ha inviato proposte al Comitato dei ministri, con l'invito ad istituire un Comitato *ad hoc* per definire il nuovo testo della Convenzione.

Oltre alla modernizzazione della Convenzione n. 108, il T-PD ha proseguito il suo lavoro sul processo di revisione delle raccomandazioni del Consiglio d'Europa, in particolare delle Raccomandazioni nn. 89(2) sulla protezione dei dati in ambito lavorativo e (87)15 sull'utilizzo dei dati a carattere personale nel settore della polizia. Anche in questi casi il T-PD, che si è avvalso della collaborazione di esperti scientifici, ha avviato una riflessione sulle strade percorribili per modernizzare tali strumenti giuridici che, pur fondati su princìpi di carattere generale tuttora validi, risentono del mutato contesto tecnologico. Con specifico riferimento alla Raccomandazione n. 89(2) sono state discusse proposte di emendamento del testo originario volte ad attualizzare il sistema di tutela dei dati personali nel contesto lavorativo.

OCSE

L'Autorità ha continuato a partecipare ai lavori del WPISP (*Working Party on Information Security and Privacy*) dell'OCSE.

Nel 2012 il Garante -membro del Gruppo e riconfermato nel *Bureau* del WPISP per il 2013- ha contribuito attivamente ai lavori soprattutto in riferimento alla complessa (e ancora in corso) revisione delle linee-guida *privacy* dell'Ocse del 1980, per la quale è stata costituita un'apposita *task force* (il "*privacy Volunteer Group* del WPISP" e formata da delegazioni di diversi Paesi, tra cui l'Italia) che ha concluso la sua missione presentando le ultime versioni delle "proposte consolidate" e la bozza di "documento supplementare" da aggiungere all'*explanatory memorandum* (originalmente allegato alle linee-guida *privacy*). In particolare le "proposte consolidate" specificano una serie di nuovi princìpi e definizioni da aggiungere ai princìpi base delle linee-guida (*accountability*; *data security breach*; *privacy by design* e *by default*; modernizzazione dei flussi transfrontalieri di dati personali; interoperabilità tra gli strumenti giurisdizionali dei Paesi membri; spinta all'educazione e alla consapevolezza/*awareness* di una "cultura della *privacy*"). Tutti i predetti punti delle proposte consolidate sono chiariti e commentati nel citato "documento di supplemento" all'*explanatory memorandum* (necessario

per comprendere il contesto e le ragioni degli aggiornamenti proposti). La versione rivista delle proposte di revisione e dell'*explanatory memorandum* dovrà ottenere il *placet* del WPISP per poi essere sottoposta al 65° meeting del Comitato ICCP (previsto per l'aprile 2013).

Nel 2012, sempre in tema *privacy*, sono stati, inoltre, forniti aggiornamenti sui *privacy framework* dei diversi Paesi membri e organizzazioni internazionali. È stato, infine, presentato un documento di sintesi della consultazione congiunta del WPISP e del Gruppo di esperti *ad hoc* sugli usi secondari dei dati personali relative alla salute (HCQI).

Le due riunioni del WPISP del 2012 hanno riservato grande attenzione alla *cybersecurity*. Molto interessante in tal senso è stata la presentazione del *report* rivisto dell'analisi comparativa delle strategie di *cybersecurity* di sei governi OCSE (Australia, Francia, Giappone, Spagna, UK e USA). I primi risultati ottenuti illustrano che la *cybersecurity* sta diventando una priorità nazionale e molti sono i punti condivisi (rafforzare il coordinamento delle *policy* e degli aspetti operativi; caldeggiare la cooperazione tra pubblico e privato; promuovere la cooperazione internazionale di *cybersecurity*). Sul punto i rappresentati dell'industria hanno chiesto che anche i prodotti per la *cybersecurity* siano pensati e condivisi a priori e non solo con l'emergere dei problemi di sicurezza. Lo studio è stato, quindi, un importante elemento di riferimento per la revisione delle linee-guida per la sicurezza delle reti del 2002 (*Guidelines for the security of Information Systems and Networks*) e la compilazione del relativo questionario. Dalle risposte del questionario è emerso che le indicazioni contenute nelle suddette linee-guida vanno rafforzate, pur mantenendone la flessibilità ed il carattere tecnologicamente neutro. È stata, inoltre, condivisa la proposta di inserire il testo della raccomandazione 2008 per la protezione delle infrastrutture critiche nel testo delle linee-guida sicurezza, per accrescere la visibilità della raccomandazione e, al tempo stesso, la completezza delle *Security Guidelines*.

Ampiamente discussi nel 2012 anche i temi legati all'impatto economico della protezione dati. In proposito, si segnala il *report Economics of Personal Data* preparato dal WPISP e dal WPIE (*Working Party on the Information Economy*), che analizza come la protezione dati comporti un valore economico e sociale che si declina in vari aspetti: dalla gestione della *supply chain* al *design* del prodotto, dalla valutazione del rischio *privacy* all'investimento nella

sicurezza. La discussione si è in particolare concentrata sull'utilizzo ed il valore dei dati nel settore privato e sull'emergere di nuove e specifiche professionalità della *privacy*.

Infine il WPISP ha affrontato il *dossier* relativo all'adesione della Russia al Gruppo stesso. Il processo di valutazione della compatibilità dell'apparato legislativo russo con l'*acquis* OCSE sta arrivando alla fase finale, ma le verifiche non sono ancora soddisfacenti; le questioni aperte riguardano essenzialmente un disallineamento nelle politiche della sicurezza dell'informazione e della *privacy*. È pertanto stata inviata una lettera dal *Chair* del WPSIP alla delegazione Russa in cui sono state indicate chiaramente le aree di preoccupazione, sulle quali si chiede alla Russia di manifestare il proprio impegno e di definire delle scadenze.

Accountability Project

L'*Accountability Project Phase* IV ha sviluppato nel 2012 la quarta fase del lavoro iniziato nel 2009 dal gruppo trasversale di esperti (provenienti tra l'altro dal mondo istituzionale, industriale, accademico) del cd. "*Galway project*" (OCSE e *Centre Information Policy Leadership Hunton & Williams LLP*), avente ad oggetto la "*Global Discussion on the commonly-accepted elements of privacy accountability*", ossia una discussione generale sugli elementi comunemente accettati di *privacy accountability* che ogni titolare del trattamento deve considerare.

Tra i principali argomenti discussi nel corso dell'anno rientrano le aspettative per un "*comprehensive programs and organisation self-assessments*", con particolare riferimento alla guida fornita dall'Autorità di protezione dati francese (CNIL) in materia di *Binding corporate rules* (*Bcr*) e al modello di *Bcr* dell'APEC; la valutazione dei rischi di *privacy* (e i conseguenti danni) che le società possono creare quando trattano dati personali; l'*accountability* per facilitare la "interoperabilità globale".

Con particolare riferimento allo sviluppo di una guida per la valutazione dei rischi di *privacy* (e dei conseguenti danni) derivanti dal trattamento di dati, il lavoro del Gruppo di esperti ha messo in luce come sia difficile trovare, a livello internazionale ed europeo, definizioni *ad hoc* e parametri condivisi sui rischi e i danni derivanti ai singoli individui (ad es., danni alla reputazione di una persona o alla dignità). I partecipanti al progetto hanno ritenuto preferibile concentrarsi sulla prevenzione del rischio, piuttosto che sui rimedi (con i conseguenti costi legali e risarcimento danni). A tal fine, un approccio di *privacy by design*

potrebbe essere promosso sulla base di metodi che prendano in considerazione una vasta costellazione di rischi per la *privacy* (materiali e immateriali), in linea con la prospettiva seguita nell'elaborazione del regolamento europeo sulla protezione dati. Il Gruppo di esperti ritiene che un approccio basato sul rischio (*risk-based approach*) sia necessario per quanto riguarda gli adempimenti di responsabili e incaricati del trattamento, ma che occorre definire con maggiore precisione i criteri utili a stabilire il livello di rischio e a compiere la difficilissima operazione di quantificare il danno su una scala di massimo/minimo livello in relazione ai diversi *data breach.*

Pertanto, il Gruppo ha deciso di elaborare nel 2013 linee-guida internazionali sulla catalogazione dei rischi e relativi danni, distinguendo tra: rischi tangibili (minacce alla vita e al benessere fisico; perdita di libertà di movimento; minacce alla vita familiare; perdita o danni ai mezzi di sussistenza; danni finanziari); rischi morali, ovvero non tangibili (ansia per la vita familiare e le relazioni sociali; ansia da intrusioni ingiustificate, violazioni della confidenzialità o altre interferenze alla liberta e all'autonomia personale; danni alla reputazione e discriminazioni non giustificabili); diniego dei diritti degli interessati alla conoscenza e all'accesso ai dati; rischi ai valori democratici e sociali di una società libera (raccolta e distribuzione delle informazioni personali non controllata; inaccettabili livelli di interferenze governative; inaccettabili livelli di interferenze commerciali; potere eccessivo della polizia e della pubblica sorveglianza; perdita di fiducia nella famiglia, amici, vicini colleghi di lavoro).

Incontri con le delegazioni estere

L'Autorità ha proseguito la sua attività nell'ambito dei programmi IPA, TAIEX e Twinning della Commissione europea rivolti ai Paesi neo-comunitari (entrati nell'UE in seguito agli allargamenti del 2004 e del 2007), ai Paesi candidati (Turchia, Croazia ed *ex* Repubblica Jugoslava di Macedonia), ai Paesi dell'area balcanica, nonché alla Russia e ai Paesi rientranti nella politica europea di vicinato, per facilitare l'avvicinamento delle normative di tali Paesi al quadro comunitario in materia di protezione dei dati.

La collaborazione con l'Autorità macedone risale al 2008, anno in cui è stato firmata una dichiarazione di mutua cooperazione. Sulla base di tale documento, oltre al programma TAIEX, si sono svolte nel marzo 2012 le attività relative ad un progetto IPA "*Support to the*

Directorate for Personal Data protection" presso l'Autorità macedone di protezione dati che hanno coinvolto funzionari del Garante in qualità di esperti sulla protezione dati in ambito Schengen -con particolare riguardo agli ambiti di polizia e giustizia. Sempre al fine di approfondire le tematiche di protezione dati nel settore polizia e giustizia nell'ambito del programma TAIEX è stata svolta una visita-studio da parte di tre funzionari del Ministero dell'interno della Repubblica di Macedonia presso il Garante, in collaborazione con il Ministero dell'interno italiano.

Quanto alla collaborazione con la Croazia, il Garante ha inviato propri esperti ai seminari TAIEX, che si sono svolti in Croazia nel dicembre 2012, riguardo ai compiti del *data protection officer*. Si è, invece, svolto presso il Garante nell'aprile 2012 l'incontro con alcuni funzionari dell'Autorità di protezione dati croata nell'ambito del progetto Twinning "*Capacity building of the Croatian Paying Agency*"; durante la visita è stato fornito un quadro generale della struttura, dell'organizzazione, dei compiti e delle modalità operative del Garante. Al contempo si è offerta una più approfondita disamina delle norme e procedure di interesse dell'Autorità croata, quali l'esercizio del diritto di accesso dell'interessato e degli altri diritti collegati, le modalità di ricorso, gli aspetti relativi all'attività di supervisione e controllo svolta dal Garante.

22. Le attività di comunicazione, studio e ricerca

22.1. La comunicazione del Garante: profili generali

Nel 2012 l'attività di informazione e comunicazione dell'Autorità ha dato particolare rilievo ai provvedimenti di maggiore interesse sociale ed economico: si pensi al funzionamento dell'Anagrafe dei rapporti finanziari collegata alla lotta all'evasione fiscale; alla trasparenza *online* della p.a.; all'uso dei dati personali a fini elettorali; all'utilizzo di *smartphone* e internet a scuola; al *telemarketing*; alla nuova realtà tecnologica del *cloud computing* nell'amministrazione pubblica e nel mondo delle imprese; al controllo dei lavoratori; alla sanità e alla ricerca medica.

Diffusa informazione è stata inoltre fornita sull'impegno dell'Autorità nei confronti del mondo della rete in relazione a temi quali la gestione e la sicurezza dei dati *online*; la tutela degli utenti dei *social network*; il *cyberbullismo* e la tutela dei minori nella rete; i nuovi servizi offerti in internet; i *blog* e i *forum* dedicati alla salute; la trasparenza nell'uso dei *cookies* e le politiche di *privacy* di Google. Anche il settore delle tlc è stato oggetto di interventi significativi, di cui si è data ampia notizia, in particolare riguardo alla sicurezza delle banche dati, all'obbligo di notificare i cd. "*data breach*", alla conservazione dei dati di traffico.

Costante è stato l'impegno nel promuovere il giusto equilibrio nel delicato rapporto tra diritto di cronaca e diritti fondamentali della persona, innanzitutto per quanto concerne il rispetto del principio di essenzialità dell'informazione. Centrale è rimasta, in questo senso, nell'attività di comunicazione l'attenzione alla tutela della riservatezza e della personalità dei minori e della dignità delle persone, specie se sofferenti.

Oltre che di tali questioni, il Servizio relazioni con i mezzi di informazione si è occupato della diffusione delle notizie riguardanti le modifiche apportate al Codice in materia di protezione dei dati personali e dell'avvio della discussione per l'adozione di una nuova normativa in materia di protezione dei dati personali a livello europeo.

In tutti questi settori, l'Autorità ha cercato di fornire, oltre ad una accurata e costante informazione, anche contributi esplicativi ed indicazioni operative per la corretta attuazione delle norme. La scelta di adottare uno stile di comunicazione e divulgazione delle notizie

semplice e al contempo rigoroso ha avuto sempre come obiettivo quello di favorire e accrescere la cultura della riservatezza e della protezione dei dati, come valore di libertà per l'individuo e la società nel suo complesso.

Lo sforzo di potenziamento nella divulgazione ha trovato un suo momento significativo con l'attivazione del nuovo sito istituzionale dell'Autorità, realizzato nel rispetto dei più avanzati criteri in materia di comunicazione istituzionale e dei necessari requisiti di usabilità e accessibilità. Per venire incontro alle esigenze di tutti gli utenti, il sito è dotato di due nuovi percorsi tematici: "Diritti e prevenzione" e "Doveri e responsabilità" che consentono un immediato e semplice accesso alle informazioni relative sia ai diritti riconosciuti ai cittadini e alle forme di tutela della propria *privacy*, sia agli obblighi che sono tenuti a rispettare quanti raccolgono, usano e conservano dati personali altrui. Un potente motore di ricerca di tipo semantico permette di effettuare ricerche estremamente mirate. Ad ogni documento vengono attribuite delle "etichette" elaborate sulla base di relazioni logico-giuridiche tra i provvedimenti, consentendo l'aggregazione trasversale di contenuti simili a quelli richiesti, rendendo così possibile la costruzione di itinerari di navigazione personalizzati.

Il sito è integrato, inoltre, da percorsi tematici, nuovi prodotti informativi (notiziario internazionale e una selezione di giurisprudenza), nuovi contenuti editoriali multimediali elaborati dal Servizio per le relazioni con i mezzi di informazione (quali video-*tutorial* e *vademecum* tematici) e sistemi di interconnessione con i principali *social network*. È stato anche avviato un canale Youtube che raccoglie e promuove i video informativi prodotti dal Garante.

L'interesse dei *media* per le tematiche riguardanti la protezione dei dati personali e l'attività del Garante è rimasto stabile rispetto allo scorso anno. Nel 2012 il competente Servizio dell'Autorità ha selezionato 33.853 articoli di interesse. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali -locali e *online*- che hanno dedicato spazio alle questioni legate generalmente alla *privacy* sono state circa 11.820, delle quali oltre 3.400 dedicate esclusivamente all'attività del Garante. Le prime pagine riguardanti i temi della protezione dei dati personali sono state circa 700 (di cui 270 riguardanti la sola Autorità). Rilevante il numero delle interviste, degli interventi e delle

dichiarazioni pubblicate sulla carta stampata (177) o andate in onda su tv e radio nazionali e locali (35). Numerose sono state anche le citazioni relative all'attività del Garante in programmi televisivi e radiofonici nazionali (346).

22.2. PRODOTTI INFORMATIVI

L'Autorità nel 2012 ha diffuso 29 comunicati e 13 *newsletter*.

La *newsletter* del Garante consente un costante e ampio approfondimento rispetto ai principali provvedimenti adottati dall'Autorità, alla sua attività in ambito europeo e internazionale e alle varie iniziative legate alla protezione dei dati personali. Giunta al suo XIV anno di pubblicazione (per un totale di 367 numeri e di 1.276 notizie), la *newsletter* è stata rinnovata completamente, sia nella grafica che nella disposizione dei testi e viene inviata per e-mail a redazioni, professionisti, pubbliche amministrazioni, imprese e a chiunque ne faccia esplicita richiesta. A tal fine, da ottobre sul nuovo sito del Garante è stata attivata l'opzione "Iscriviti alla *newsletter*". Sul sito è inoltre possibile consultare l'archivio tematico della pubblicazione che raccoglie per categorie i 14 anni di articoli prodotti dal Servizio.

Nel 2012, è stata pubblicata la XXII edizione del Dvd "Il Garante e la protezione dei dati personali", al cui interno è disponibile un'ampia documentazione sull'attività dell'Autorità, la legislazione nazionale ed internazionale, una sezione "temi" con schede informative multimediali su argomenti di particolare interesse. Il Dvd, pubblicato ogni anno, realizzato in 5.000 copie, viene distribuito al pubblico in occasione di manifestazioni nazionali, convegni e seminari ai quali partecipa il Garante, oltre ad essere inviato a quanti ne fanno specifica richiesta. In primavera è stata inoltre realizzata la seconda edizione del Cd in lingua inglese "*Data protection in Italy and Europe*", dedicato alla normativa italiana ed europea sulla *privacy* e completamente aggiornato, sia nei contenuti che nella impostazione grafica.

22.3. PRODOTTI EDITORIALI

Proseguendo nella linea inaugurata da alcuni anni di realizzare *vademecum* su settori specifici e di particolare interesse per cittadini, istituzioni, liberi professionisti, imprese, è stata pubblicata una nuova mini guida, disponibile anche in inglese: "*Cloud computing.*

Proteggere i dati per non cadere dalle nuvole", pensata sia per gli esperti del settore, sia per coloro che sono interessati alla comprensione e alla potenziale adozione di queste nuove tecnologie, a partire dalle pubbliche amministrazioni e dalle aziende private.

Nell'imminenza dell'apertura delle scuole, il Garante ha ritenuto utile fornire a professori, genitori e studenti, sulla base dei provvedimenti adottati e dei pareri resi, alcune indicazioni generali in materia di tutela della *privacy* attraverso un *vademecum* dedicato a "La *privacy* a scuola. Dai *tablet* alla pagella elettronica".

È stata, infine, pubblicata la seconda edizione aggiornata di tutte le linee-guida adottate finora dal Garante nei diversi settori, dalla pubblica amministrazione alla sanità elettronica, dalle banche all'informazione giuridica. Le linee-guida del Garante mirano a fornire indicazioni di carattere generale in relazione al trattamento di dati personali, al fine di garantire la corretta applicazione dei princìpi stabiliti dal Codice.

22.4. GLI INCONTRI INTERNAZIONALI

La consueta Conferenza internazionale dei Garanti per la *privacy* nel 2012 si è svolta a Punta del Este, in Uruguay, dal 23 al 24 ottobre. La sfida sulla quale si sono confrontati i Garanti del mondo durante i due giorni di lavori della 34ª edizione dell'*International Conference of Data Protection* è stata quella di dimostrare che lo sviluppo tecnologico e la protezione dei dati personali non sono in contrasto tra loro, ma possono e devono trovare un giusto equilibrio nell'individuare approcci e soluzioni. Attraverso sessioni plenarie -su temi globali quali gli ultimi sviluppi tecnologici, l'*e-government*, le soluzioni normative in Europa e nel mondo-, e gruppi di lavoro dedicati ad approfondire alcune fra le problematiche più scottanti (trasparenza e riutilizzo delle informazioni pubbliche, geolocalizzazione, sanità elettronica, tecnologie mobili, *marketing* e profilazione, proprietà intellettuale, e, non da ultimo, il bilanciamento dei diritti fondamentali), i rappresentanti delle autorità mondiali, *manager* di multinazionali ed esperti del settore hanno analizzato e definito linee di sviluppo per prospettare approcci, quanto più possibile, condivisi.

All'Autorità italiana, rappresentata dal Segretario generale Giuseppe Busia, è stato affidato il compito di affrontare il tema del necessario bilanciamento fra il diritto fondamentale alla

protezione dei dati e la libertà di informazione ed espressione, in una sessione che ha visto contributi provenienti dalle due sponde dell'Atlantico.

22.5. LE MANIFESTAZIONI E LE CONFERENZE

L'attività di divulgazione dell'Autorità, realizzata attraverso la partecipazione dei componenti del Collegio e dei dirigenti a seminari, convegni ed altre iniziative, anche nel 2012 ha riscontrato vivo interesse da parte del pubblico.

Come consuetudine l'Autorità ha partecipato alla XXIII edizione del *Forum Pa* svoltasi a Roma dal 16 al 19 maggio 2012 e dedicata al tema: "Agenda digitale semplificazioni e sviluppo nell'*open Government*".

Nell'ambito della manifestazione, il Garante ha affrontato i temi legati alla protezione dei dati personali rispetto a questioni rilevanti come la trasparenza della p.a., le semplificazioni, l'interoperabilità dei sistemi, le grandi banche dati, il *cloud computing*.

Francesco Pizzetti, Presidente dell'Autorità fino a giugno, è intervenuto, in una delle sessioni, sul tema della nuova società dell'informazione e sulla necessità di conciliare il diritto alla trasparenza ed efficienza della p.a. con il diritto alla tutela della riservatezza dei dati personali. Alcuni dirigenti dell'Autorità sono invece intervenuti nell'ambito dei convegni organizzati su "Soluzioni e *Governance IT* nell'era del *Cloud*", "Lo stato dell'arte dell'operazione trasparenza" e "*Cloud computing* per la sanità digitale".

Durante i quattro giorni della manifestazione, il personale incaricato ha risposto a quesiti e distribuito le pubblicazioni curate dall'Autorità al numeroso pubblico che si è soffermato presso lo *stand* istituzionale del Garante.

A Torino, sempre a maggio, nell'ambito della 25ª edizione del Salone internazionale del libro, il Presidente Pizzetti ha tenuto una *lectio magistralis* dal titolo "Controllo dei dati e diritto alla riservatezza". Nel 2012, prima di lasciare l'incarico, il Presidente ha partecipato a numerosi altri incontri, tra i quali il convegno organizzato dalla Luiss su "Informazione e giustizia, come conciliare rispetto della *privacy* e libertà di stampa?" e quello su "Politica e *privacy* tra diritto di cronaca e diritto alla riservatezza", organizzato presso la Camera dei deputati.

Antonello Soro, da giugno Presidente del nuovo Collegio, ha avuto modo di presentarsi al vasto pubblico intervenendo a diversi incontri. Ad ottobre ha partecipato, in qualità di relatore, al X Rapporto sulla comunicazione "I *media* siamo noi. L'inizio dell'era biomediatica" organizzato dal Censis. A novembre, la tavola rotonda sulle "*Authority* nazionali ed europee: prospettive per la tutela dei cittadini" organizzata da *Consumers' Forum*, è stata un'occasione per fare un bilancio delle attività di tutte le autorità indipendenti. Il Presidente Soro, in quell'occasione, ha affrontato il tema delle grandi banche dati pubbliche e private e dei rischi per la riservatezza dei cittadini che possono derivare da una non adeguata protezione dei dati personali.

Il Presidente è intervenuto anche alla IV edizione del Premio "Nostalgia di futuro" -organizzato dall'Associazione *Media* Duemila in collaborazione con Fieg e OsservatorioTutti*Media*"- quest'anno dedicato a "La persona digitale: *privacy* e regole nell'era dei *social media*". In quell'occasione Soro ha affermato che i dati personali sono come le tessere di un mosaico che rappresentano e descrivono la nostra identità. Ogni giorno navigando in rete o utilizzando i *social network* spargiamo dettagli importanti della nostra biografia, anche la più intima, che rimarranno nell'enorme spazio pubblico che è la rete per molto tempo, se non per sempre. Sarebbe per questo auspicabile, secondo Soro, la definizione di una Costituzione mondiale per internet che consenta di proteggere ovunque la propria identità digitale.

Il 28 gennaio 2013 è stata celebrata la Giornata Europea della protezione dei dati personali. A partire dal 2007 questo è il giorno scelto per ricordare la data dell'adozione della Convenzione di Strasburgo n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati. Si tratta di un'iniziativa promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità europee per la protezione dei dati personali, con l'obiettivo di informare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante italiano ha voluto dedicare la Giornata al delicatissimo tema del *cyberbullismo,* chiamando a discuterne insieme il mondo della scuola e quello dei *social network*, al fine di sensibilizzare i giovani sui pericoli di un uso poco attento o responsabile delle nuove forme di comunicazione.

Il tema è stato trattato nell'ambito della trasmissione "Uno Mattina" della Rai Radiotelevisione italiana ed ha visto la partecipazione in studio del Presidente dell'Autorità Antonello Soro insieme al Ministro dell'istruzione Francesco Profumo e ad un responsabile di Google Italia.

In occasione della Giornata Europea il Garante ha inoltre lanciato una campagna informativa rivolta ai giovani e messo a disposizione sul proprio sito web istituzionale un video *tutorial* con le istruzioni per un uso consapevole dei *social network* e un *test* con venti semplici domande per verificare il grado di conoscenza dei principali rischi che si possono correre in rete.

22.6. LE RELAZIONI CON IL PUBBLICO

Anche nel 2012 l'Autorità ha quotidianamente garantito, attraverso l'Ufficio relazioni con il pubblico, un servizio di comunicazione istituzionale, anche *online,* basato sulla correttezza nel rapporto fra pubblica amministrazione e cittadino, in linea con il principio di trasparenza amministrativa introdotto dalla l. 7 agosto 1990, n. 241.

Come rappresentato nelle precedenti edizioni, l'Ufficio relazioni con il pubblico costituisce il luogo deputato all'interazione fra le istanze del cittadino e le risposte dell'Autorità nonché alla partecipazione diretta all'attività amministrativa attraverso le varie modalità della comunicazione istituzionale.

L'azione dell'Urp, attraverso il continuo dialogo fra *input* ricevuti e *output* restituiti all'utenza, realizza inoltre una costante attività di *testing* in relazione all'efficienza dell'Autorità e al livello di soddisfazione testimoniato dal cittadino.

Le numerose istanze ricevute vengono trattate e riscontrate con rapidità, spesso in tempo reale, attraverso procedure snelle volte a privilegiare forme di comunicazione diretta. Vengono inoltre forniti chiarimenti sulle tematiche oggetto dei quesiti ricevuti, ponendo sempre grande attenzione agli aggiornamenti delle disposizioni sulla protezione dati alla luce del più ampio contesto normativo.

L'Ufficio svolge altresì un importante ruolo informativo interno attraverso la segnalazione degli *input* ritenuti d'interesse -spesso oggetto di vivaci dibattiti sui *media*- contribuendo al

miglioramento dell'attività interna a beneficio del diritto del cittadino alla trasparenza e all'efficienza dell'Autorità.

L'attività dell'Ufficio relazioni con il pubblico

L'attività dell'Urp è stata imperniata sull'analisi delle richieste provenienti dai cittadini e la conseguente elaborazione di soluzioni proposte con prontezza, di regola attraverso strumenti immediati quali sono le comunicazioni via e-mail o telefoniche; tali modalità organizzative e procedimentali hanno comportato di massima la sostanziale contestualità di *input* ricevuti e *output* restituiti.

Le diverse funzioni svolte dall'Ufficio relazioni con il pubblico sono riconducibili a tre macro-aree:

- orientamento: dopo aver indicato, ove possibile, un provvedimento generale quale precedente adottato in materia dall'Autorità o avere trasmesso note tipo e/o modelli di istanza appositamente predisposti, viene offerto al cittadino un servizio volto alla individuazione dello strumento di tutela più adatto al caso di specie;

- interazione nei rapporti con l'utenza: le segnalazioni e le sollecitazioni di maggiore rilievo divengono oggetto di interventi mirati da parte dell'Autorità;

- informazione al cittadino: viene offerto un rapporto diretto e dedicato presso la sede del Garante ovvero mediante mezzi di comunicazione quali il contatto telefonico o la posta elettronica. Particolarmente apprezzato dall'utenza è stato anche il servizio di guida alla navigazione del sito istituzionale dell'Autorità, soprattutto dopo le novità intervenute a partire dal suo recente *restyling*.

Anche nel trascorso anno di attività, l'Ufficio ha potuto registrare frequenti attestazioni di gradimento per il servizio erogato, confermando il positivo *trend* nel riscontro dei cittadini. Per migliorare il servizio, l'Urp sta predisponendo una scheda da pubblicare sul sito del Garante per raccogliere le valutazione e le indicazioni degli utenti.

Numerose sono state le richieste di intervento in relazione all'attività di *marketing* cd. "selvaggio", e, in particolar modo al *direct marketing*, soprattutto telefonico, di cui più diffusamente si dà conto *infra* con le altre tematiche di interesse (cfr. *supra* par. 11.).

Con specifico riferimento alle telefonate promozionali, ma anche sulle più variegate tipologie di quesiti, l'Urp ha prestato un'assistenza a 360°, che ha inizio con la valutazione

dei presupposti delle iniziative e prosegue sino all'inoltro dell'istanza formale da parte dell'interessato all'Autorità.

Tale attività di supporto è stata realizzata verificando costantemente, attraverso il Dipartimento competente, la sussistenza dei requisiti formali e sostanziali per l'intervento dell'Ufficio. Un ruolo di informazione nei confronti dell'utenza è stato svolto anche in pendenza del procedimento amministrativo presso l'Autorità (dalla semplice richiesta di conoscere lo stato dell'istruttoria alla richiesta di accesso agli atti ai sensi della l. n. 241/90).

L'analisi complessiva dei dati statistici conferma che l'attenzione dei cittadini in merito alla sfera della riservatezza personale e alla protezione dei dati è in costante crescita. Nell'ambito dell'attività di *front office*, infatti, i contatti registrati nel periodo di riferimento sono complessivamente pari a 34.660 (contatti telefonici, e-mail, visitatori, fascicoli), di cui oltre 33.969 a mezzo del telefono e della posta elettronica. A questi dati vanno aggiunti 254 fascicoli trattati nel 2012.

In particolare, i contatti avvenuti attraverso il *call center* o direttamente ai numeri di telefono messi a disposizione dei cittadini (anche mediante diffusione sul sito web istituzionale) sono stati circa 15.000.

Gli utenti hanno altresì manifestato gradimento per l'attività di ricevimento diretto, che ha interessato circa 437 unità: laddove possibile, questa modalità di contatto consente la contestuale distribuzione di materiale informativo e di documentazione.

La trattazione degli oltre 19.000 quesiti giunti per e-mail e posta ordinaria è avvenuta nella gran parte dei casi in tempi decisamente spediti (1-2 giorni lavorativi).

L'analisi dei dati elaborati consente peraltro non solo l'esame della tipologia delle richieste, ma anche l'identificazione dei diversi *target* dell'utenza che vi si rivolge. Ne è conseguenza l'elaborazione di un *output* modulato sulle caratteristiche dell'istante, sia esso un soggetto pubblico, un consulente dotato di competenze tecniche ed esigenze specifiche, o un privato cittadino.

È stata confermata nel periodo di riferimento la tendenza all'instaurarsi di un rapporto continuativo tra certe categorie di utenti e Urp: sovente, infatti, al primo contatto ne sono seguiti altri, mirati all'approfondimento della conoscenza di norme e provvedimenti dell'Autorità.

Un'attenzione particolare è riservata al perfezionamento di procedure di gestione delle emergenze, garantendo la comunicazione immediata ai dipartimenti competenti e, qualora necessario, al vertice istituzionale.

Tematiche d'interesse

Dall'analisi delle segnalazioni e dei contatti telefonici con l'Urp, si conferma una generale informazione e consapevolezza dei propri diritti, testimoniate dal contenuto definito e circostanziato delle richieste nonché dal numero consistente delle sollecitazioni sull'argomento. Anche nell'anno di riferimento, quindi, una consistente parte dell'attività, è stata dedicata alla selezione e prima analisi delle segnalazioni pervenute (4.491 e-mail), per verificare la completezza dei presupposti per la trattazione, ovvero per richiedere agli interessati l'integrazione degli elementi necessari per l'inoltro ai Dipartimenti competenti per l'istruttoria e la redazione dei provvedimenti, anche di natura sanzionatoria.

Anche nel 2012, il *marketing* telefonico è stato l'argomento sul quale è pervenuto il maggior numero di richieste (24%) in linea con il *trend* dello scorso anno, nel quale è entrata a regime, con il Registro pubblico delle opposizioni, la nuova disciplina giuridica dei dati pubblicati negli elenchi telefonici in relazione all'utilizzo per finalità promozionali e pubblicitarie (d.P.R. 7 settembre 2010, n. 178) (v. Relazione 2011 p. 100 e ss.). Va al riguardo confermato che -a seguito dell'istituzione del predetto Registro- il *marketing* selvaggio non è stato arginato, ed in diversi casi è risultato particolarmente invasivo, suscitando l'esasperazione dei cittadini che si erano tempestivamente iscritti nel Registro.

Di forte impatto sugli interessati altresì il recente fenomeno delle cd. "telefonate mute", oggetto di numerose segnalazioni (cfr. *supra* par. 11.3.).

Rispetto all'anno precedente, la percentuale di richieste di intervento in materia di attività di *marketing* svolte attraverso altri canali, quali la posta cartacea, le e-mail e i fax pubblicitari indesiderati, è rimasta invariata (14%). In relazione a questo tema, l'Ufficio ha svolto un'attività analoga a quella sopra descritta, concernente, in particolare, 2.617 segnalazioni di ricezione di e-mail e fax indesiderati.

Anche in altre aree tematiche si è registrato un consolidamento del numero di segnalazioni/richieste di informazioni in percentuale sul totale. Rappresentano ciascuna una quota tra il 3 e il 4% del totale le questioni relative alla videosorveglianza, al trattamento dei

dati personali nella gestione del rapporto di lavoro, all'ambito giornalistico (anche *online*), ai gestori telefonici, alla trasparenza amministrativa e alla pubblicazione *online* di dati personali da parte di enti locali.

Il consistente numero di richieste di informazioni e di segnalazioni in materia di videosorveglianza (827 e-mail) testimonia la crescente diffusione, anche in Italia, di questa tipologia di dispositivi, tanto nel settore pubblico quanto in quello privato, in ambito sia aziendale sia domestico. Le richieste riguardano principalmente alcuni adempimenti previsti dal provvedimento generale in materia [doc. web n. 1712680], con particolare riferimento alla richiesta di verifica preliminare (art. 17 del Codice) ed alle misure di sicurezza (artt. 31-36 e Allegato B. del Codice). In ambito pubblico molte richieste riguardano la rilevazione di infrazioni al codice della strada, l'accesso ai centri storici ed alle ztl, le funzioni di sicurezza pubblica assegnate ai comuni mentre, nel settore privato, attengono all'utilizzo di questi dispositivi in ambito lavorativo (controllo a distanza), nel condominio, e all'uso per fini personali ovvero a presidio della sicurezza dell'abitazione privata (spesso non rientrante nell'ambito di applicazione del Codice).

Risultano ricorrenti anche le tematiche relative al trattamento dei dati nella gestione del rapporto di lavoro (721 e-mail), sia in ambito pubblico che alle dipendenze di aziende private, tanto da parte dei lavoratori quanto da parte datoriale, che riguardano il trattamento di dati biometrici, la diffusione di dati personali dei lavoratori in bacheche aziendali o sul web, l'utilizzo delle risorse elettroniche aziendali (internet e posta elettronica), il controllo a distanza, la geolocalizzazione e l'utilizzo di dispositivi *Gps* sui mezzi aziendali, il trattamento dei dati relativi allo stato di salute del lavoratore o di suoi familiari, il trasferimento di dati all'estero.

Nel settore pubblico è oggetto di interesse soprattutto l'attuazione del nuovo quadro giuridico sulla trasparenza e la pubblicazione di documenti da parte delle pp.aa. (572 e-mail), principalmente attraverso i siti istituzionali, ma anche attraverso altre modalità (bollettini, albi e bacheche). Sempre in conseguenza della maggiore trasparenza richiesta alle pubbliche amministrazioni, numerosi chiarimenti hanno riguardato la registrazione audio-video delle sedute dei consigli comunali, nonché la possibilità di una successiva diffusione sia nel sito

istituzionale dell'ente, sia in siti di privati cittadini o gruppi politici. Continuano, inoltre, a pervenire numerose richieste di parere in materia di accesso -sia da parte dei cittadini, sia da parte dei consiglieri comunali- a documenti amministrativi di enti locali per le quali, come noto, la competenza spetta anzitutto all'amministrazione destinataria delle istanze.

Considerati i frequenti interventi dell'Autorità nel trattamento dei dati personali nell'ambito dell'attività giornalistica, risultano numerose le istanze dell'utenza volte ad ottenere chiarimenti, ma anche a sottoporre delle segnalazioni. Come negli anni precedenti, per la diffusione delle testate giornalistiche *online* la maggior parte dei quesiti e delle richieste di chiarimenti riguarda il corretto esercizio del diritto di cronaca ed il diritto all'oblio in internet, nonché l'indicazione di strumenti di tutela adeguati ai singoli casi sottoposti (cfr. *supra* par. 9.).

Con riferimento al sempre più pervasivo uso delle tecnologie e di internet, numerose criticità sono state segnalate in relazione alla protezione dei dati personali nei *social network* (Facebook, MySpace,…), anche, ma non solo, da parte di utenti di giovane età.

Le segnalazioni e richieste relative al settore del credito complessivamente rappresentano circa il 6% del totale delle istanze pervenute all'Urp. Quelle in ambito bancario (407 e-mail) riguardano la pertinenza e non eccedenza delle informazioni richieste dalle banche, rispetto alla valutazione sull'adeguatezza e appropriatezza delle operazioni e dei diversi servizi di investimento forniti o sull'applicazione della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231), le modalità di identificazione agli sportelli, le comunicazioni a terzi di informazioni bancarie, l'ambito applicativo del diritto di accesso ai propri dati personali nonchè il diverso diritto di accesso alla documentazione bancaria (art. 119 d.lgs. n. 385/1993, testo unico delle leggi in materia bancaria e creditizia) (v. al riguardo par. 18.5.). Relativamente all'attività di recupero crediti (436 e-mail), continuano ad essere segnalate modalità di contatto molto invasive e lesive della riservatezza e della dignità personale, quali visite al domicilio o sul luogo di lavoro, sollecitazioni telefoniche anche presso familiari, vicini di casa, utilizzando recapiti non forniti dagli interessati. Infine, sempre nel settore del credito, continuano ad essere numerose le richieste di assistenza volte ad attivare le procedure di aggiornamento, correzione, cancellazione di dati personali trattati dai sistemi informativi privati in materia di credito al consumo e puntualità e affidabilità nei pagamenti (297 e-mail).

Altra voce significativa è risultata essere quella relativa alle richieste di informazioni sugli adempimenti previsti dal Codice (complessivamente l'8% delle e-mail trattate), sia per quanto concerne le modalità da porre in atto per esercitare gli strumenti di tutela a disposizione dei cittadini che per le misure di sicurezza. Numerose istanze e quesiti riguardano inoltre le recenti modifiche normative apportate al Codice (con il decreto semplificazioni, d.l. 9 febbraio 2012, n. 5 convertito, con modificazioni, con l. 6 aprile 2012, n. 35 e il cd. "decreto Salva Italia", d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, in l. 22 dicembre 2011, n. 214), con particolare riguardo all'esclusione delle persone giuridiche dall'applicazione del Codice.

22.7. SERVIZIO STUDI E DOCUMENTAZIONE

La redazione della Relazione annuale

Il Servizio studi ha coordinato, come di consueto, la redazione del testo della Relazione annuale per la presentazione al Parlamento.

Si tratta, come noto, di un fondamentale adempimento istituzionale dell'Autorità, divenuto nel tempo un'importante occasione di riflessione e analisi interna sull'attività svolta, anche ai fini della programmazione e dei possibili miglioramenti nello svolgimento delle funzioni del Garante, tra le quali quella di curare, anche attraverso il sito istituzionale, la conoscenza da parte del pubblico della disciplina in materia di trattamento dei dati.

La funzione di studio e di supporto giuridico

Il Servizio studi ha svolto studi e ricerche su questioni tecnico-giuridiche di interesse dell'Autorità, anche su impulso del Collegio, del Segretario generale nonché delle strutture dell'Ufficio.

In particolare sono stati svolti approfondimenti sull'attività di vigilanza sul funzionamento del registro pubblico delle opposizioni alle chiamate telefoniche promozionali, ai sensi dell'art. 130, comma 3-*quater* del Codice; sulle proposte di modifica della normativa comunitaria in materia di protezione dei dati personali, con specifico riguardo all'accesso a documenti pubblici; sul trattamento dei dati personali da parte delle persone giuridiche negli ordinamenti europei e sull'accesso da parte di un consigliere regionale ai dati contenuti nella cartella clinica di una persona sottoposta a trattamento sanitario obbligatorio. È stata ulteriormente esaminata la questione dell'applicabilità dell'istituto della *prorogatio* al Collegio del Garante, poi affermativamente risolta con parere del Consiglio di Stato (n. affare 03608/2012).

Inoltre l'attività istituzionale del Garante è stata coadiuvata, attraverso la ricerca e la trasmissione alle strutture interessate, di documentazione nonché di sintetiche osservazioni su questioni d'interesse, quali le sanzioni per il trattamento illecito dei dati (art. 167 del Codice), i profili relativi alla protezione dei dati connessi alla funzionalità del servizio *Google web search*, il rapporto del *Joint Committee* della Camera dei *Lord* e della Camera dei Comuni su *privacy* ed ingiunzioni.

Sono stati altresì forniti alla Segreteria generale materiale utile ed elementi di riflessione in vista della 34ª Conferenza internazionale dei Garanti per la *privacy*, svoltasi in Uruguay nel mese di ottobre.

I pareri sulle leggi regionali

Il Servizio ha costantemente fornito, a mezzo di atti interni, elementi di valutazione su leggi regionali, ai fini della formulazione dei pareri richiesti dalla Presidenza del Consiglio dei ministri, per l'eventuale impugnazione davanti alla Corte costituzionale, ai sensi dell'art. 127 Cost.. Le menzionate valutazioni attengono, previ approfondimenti normativi, giurisprudenziali ed eventualmente dottrinali, alla conformità delle leggi regionali alla disciplina sulla protezione dei dati personali (cfr. *supra* par. 3.4.).

Come negli anni precedenti, i testi legislativi esaminati sono risultati, di massima, rispettosi dei limiti di cui all'art. 117 Cost., anche alla luce di quanto deciso dalla Consulta (sentenza n. 271/2005) sulla competenza legislativa esclusiva dello Stato in materia di *privacy*, nonché dei princìpi e delle disposizioni contenuti nella normativa internazionale (art. 8 CEDU) e comunitaria.

Al riguardo tra i testi più significativi si cita una legge in materia di registro regionale di dialisi e trapianto, ritenuta conforme alla normativa in materia di protezione dei dati personali anche in ragione di considerazioni relative ai margini entro i quali, solo ed in quanto previsto dalla legislazione statale, possano essere adottati atti normativi regionali, di natura meramente integrativa.

Oggetto di approfondimento è stata altresì una legge regionale in materia di anagrafe pubblica degli eletti e dei nominati che ha, in particolare, disposto la pubblicità della dichiarazione dei redditi e della situazione patrimoniale dei componenti dell'Assemblea legislativa, della Giunta e degli eventuali conviventi *more uxorio* nonché la pubblicazione, a

mezzo di diffusione sui siti internet, dei lavori assembleari, ivi compresi gli ordini del giorno, i verbali e le registrazioni audio. Al riguardo la pressoché indiscriminata diffusione di una molteplicità di informazioni comprensiva astrattamente di dati sensibili, in ragione delle competenze dei menzionati organi collegiali, è apparsa di dubbia conformità ai princìpi di pertinenza e di non eccedenza di cui all'art. 11 del Codice, alla disciplina sul trattamento dei dati sensibili nonché ai princìpi indicati dalla Corte di giustizia europea, secondo la quale "*Si deve ricordare che le istituzioni, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l'interesse dell'Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta. Orbene, non può riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali (v., in tal senso, sentenza Commissione/Bavarian Lager, cit., punti 75 79), anche qualora siano coinvolti rilevanti interessi economici*." (Grande sezione, 9 novembre 2010, in C 92/09 e C 93/09 riunite).

Si aggiunge infine, a titolo di citazione meramente esemplificativa, una legge regionale sull'ordinamento della polizia locale, il cui impianto complessivo è risultato conforme alla normativa e ai princìpi nazionali ed europei in materia di protezione dati, mentre ha sollevato dubbi una norma sulla comunicazione esterna dell'attività di polizia locale, che come unico e inderogabile limite ad ogni forma di comunicazione sulle operazioni di servizio svolte, aveva individuato il segreto istruttorio, senza alcun richiamo alle normativa sulla protezione dei dati personali.

I servizi interni di documentazione

Analogamente agli anni passati, l'aggiornamento del personale è stato curato attraverso la redazione di due notiziari interni:

- il "Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona" denominato "Osservatorio *privacy*", una rassegna periodica di normativa, dottrina e giurisprudenza nazionale comunitaria ed internazionale su questioni di interesse per l'Autorità, suddivisa in un'ampia sezione di princìpi generali e in quattro sezioni più specialistiche, corrispondenti alle macroaree tematiche di attività del Garante: libertà pubbliche e sanità; comunicazione e reti telematiche; realtà economiche e produttive; amministrazione, contratti e risorse umane;

- il "Servizio studi *news*", strumento di monitoraggio della giurisprudenza, anche comunitaria ed internazionale in materia di diritti e libertà delle persone e protezione dei dati personali. In proposito, nel richiamare quanto già osservato nella precedente Relazione circa il contesto più generale dell'attività, nel quale giudici ed autorità di sistemi giuridici diversi valutano i diversi casi alla luce di concorrenti princìpi di carattere generale, si segnala, tra i punti di riflessione emersi dall'analisi, la questione dell'ampiezza dei margini di apprezzamento di cui godono gli Stati aderenti alla Convenzione europea dei diritti dell'uomo nel bilanciamento tra il diritto alla protezione della vita privata e la libertà di espressione (artt. 8 e 10 CEDU, v. al riguardo la sentenza della *Grande Chambre* resa il 7 febbraio 2012 in *Axel Springer AG c. Allemagne*, ric. n. 39954/08, e l'opinione dissenziente ivi espressa circa i limiti dei poteri di controllo spettante alla Corte).

Nell'ultima parte dell'anno sono stati altresì organizzati seminari interni su tematiche giuridiche e tecnico-informatiche per la formazione e l'aggiornamento del personale.

22.8. BIBLIOTECA

Come segnalato nelle Relazioni degli anni precedenti, la Biblioteca nasce nel 2001 e rappresenta un'articolazione della Segreteria generale. Il suo compito istituzionale consiste nella raccolta e nella conservazione delle pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati. In raccordo con il dettato normativo, l'incremento del patrimonio della Biblioteca si estende alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale.

Il patrimonio della Biblioteca è costituito di 13.840 volumi (circa 7.000 in lingua straniera) e 400 periodici, dei quali 36 correnti (dati aggiornati al 31 dicembre 2012). La Biblioteca dispone inoltre di un fondo con ca. 200 tesi italiane di laurea e di dottorato in materia di protezione dei dati. Le nuove accessioni dello scorso anno ammontano a ca. 2.800 titoli, 1.600 dei quali pervenuti in dono (ca. 1.000 volumi sono stati donati dal Presidente uscente prof. Pizzetti) e 1.200 per acquisto.

Dal 2004 sulla rete intranet è consultabile il catalogo OPAC dei titoli posseduti, con 5.372 volumi inseriti (5.054 monografie). Gli aggiornamenti del catalogo informatizzato delle acquisizioni successive al 2004 vengono pubblicati sul sito web della Biblioteca.

In quanto specializzata nelle discipline giuridiche attinenti alla protezione dei dati, la Biblioteca svolge essenzialmente una funzione amministrativa ed agisce da supporto alle attività di informazione, di ricerca e di studio dell'Autorità.

Nel 2012 è stato completato il riordino delle collezioni e si è proceduto ad una nuova sistemazione delle sale di consultazione. Sono state istituite otto sezioni tematiche, comprendenti nell'ordine: a) la raccolta completa delle pubblicazioni a stampa dell'Autorità; b) la letteratura italiana sulla riservatezza e sulla protezione dei dati, con particolare riguardo alle pubblicazioni successive alla costituzione dell'Autorità; c) la letteratura italiana sulle autorità indipendenti; d) le pubblicazioni a stampa delle autorità sulla protezione dei dati dei Paesi membri della UE; e), f), g) e h): la letteratura mondiale sulla *data protection*, suddivisa nelle macro-aree culturali tedesca, francese, spagnola e anglo-americana.

Nella ristrutturazione delle sale è stato conferito particolare risalto alla produzione editoriale internazionale. Da questo punto di vista va osservato come il patrimonio in lingua straniera della Biblioteca costituisca una singolarità nel panorama bibliotecario italiano: ben 6.500 sui 7.000 titoli esteri delle collezioni (il 92%) non appaiono schedati nel catalogo SBN e risultano dunque reperibili soltanto presso l'Autorità.

Il progetto di *Digital Library*, avviato nel 2008 in cooperazione con il Dipartimento risorse tecnologiche, è stato arricchito con le nuove risorse di *eBook libraries* consultabili sulla rete intranet. Accanto alle "strategie di possesso" (imperniate sull'incremento del patrimonio cartaceo) sono state potenziate le "strategie di accesso" concentrate negli archivi *full-text* pubblicati in formato elettronico. Il sito web della Biblioteca, trasformato in portale, rafforza la suddivisione in aree funzionali in modo da coordinare tutte le risorse bibliografiche elettroniche (l'OPAC *online* e i *database*) nel quadro di una complessa *knowledge infrastructure*: questa architettura di conoscenze condivise riflette la *mission* della Biblioteca e fornisce una serie di strumenti qualificati per le attività del Collegio e per il lavoro dei dipartimenti e dei servizi nei rispettivi settori di competenza. L'inserimento della formula della multiutenza sulla rete intranet in luogo delle autenticazioni basate su credenziali individuali ha permesso di ottimizzare la condivisione delle risorse, aumentando il numero delle banche dati giuridiche di accesso web e di accesso remoto rese disponibili su tutte le postazioni dell'Ufficio.

Nel 2012 i documenti richiesti in lettura dagli utenti interni sono stati 4.601, 135 le domande di frequentazione di utenti esterni e 1.905 le richieste di titoli in lettura. I contatti sul catalogo OPAC sono saliti a 6.012 rispetto ai 5.800 del 2011. I casi di assistenza bibliografica e di *documents delivery* effettuati *online* sono stati 278 (231 per l'utenza esterna).

In questo quadro, i dati analitici relativi alla consultazione dei *database* giuridici da parte della utenza interna rivestono speciale importanza come indicatori dell'elaborazione che precede la messa a punto dei "prodotti" dell'Ufficio. Per quanto riguarda le quattro banche dati giuridiche commerciali di maggiore rilevanza, il numero totale dei documenti consultati ha superato i 75.000. Il *database* con il più elevato conteggio statistico ha totalizzato 5.828 sessioni di lavoro (4.889 nel 2011 e 4.052 nel 2010, con un incremento del 19% sul 2011 e del 43% sul 2010) e 60.419 documenti consultati (60.141 nel 2011 e 48.112 nel 2010), per una media giornaliera lavorativa di ca. 26 connessioni e 275 documenti.

L'Ufficio del Garante

III. L'Ufficio del Garante

23. La gestione amministrativa dell'Ufficio

23.1. Il bilancio e la gestione finanziaria

Le risorse finanziarie acquisite al bilancio del Garante sono state utilizzate per lo svolgimento dei compiti istituzionali dell'Ufficio e per il perseguimento degli obiettivi programmatici definiti in sede di approvazione del bilancio di previsione per il 2012, nel rispetto delle procedure di legge e regolamentari che disciplinano la materia.

La gestione amministrativa ha fatto registrare, per quanto attiene le entrate accertate, un sostanziale allineamento rispetto alle somme stanziate in sede di previsione, anche se non tutti gli importi sono stati riscossi nell'esercizio di competenza.

Riguardo alle uscite, il confronto dei dati consuntivi rispetto alla stima iniziale, ha evidenziato economie di gestione, realizzate anche per effetto dell'applicazione delle misure di contenimento della spesa previste sul piano legislativo a cui l'Autorità si è pienamente conformata.

Le entrate totali di cui il Garante ha acquisito il diritto alla riscossione nell'anno 2012 sono state pari complessivamente a 23,6 milioni di euro, in lieve flessione rispetto al precedente esercizio (23,8 milioni) essenzialmente per una generale riduzione dei rimborsi provenienti da altre amministrazioni, in funzione delle spese anticipate dall'Autorità per il proprio personale destinato a prestare servizio presso altri soggetti pubblici.

Le somme spettanti sono state in massima parte incassate nell'anno e soltanto una parte limitata è stata acquisita tra la fine dell'esercizio ed i primi mesi del nuovo anno.

La fonte di finanziamento maggiormente significativa, che ha peraltro consentito di assicurare il necessario equilibrio finanziario, è rappresentata dal contributo posto a carico di altre autorità amministrative indipendenti, il cui importo annuo è quantificato nella misura complessiva di 12,0 milioni di euro, *ex* art. 1, comma 241, della l. 23 dicembre 2009, n. 191. Tale disposizione, limitata inizialmente soltanto agli anni 2011 e 2012, è stata recentemente prorogata in favore del Garante per ulteriori tre anni con effetti a partire già dal corrente esercizio finanziario 2013.

Per quanto attiene, invece, allo stanziamento erariale assicurato annualmente in tabella C dalla legge di stabilità, il raffronto con il precedente anno ha fatto segnare un incremento di 0,3 milioni di euro. Il saldo positivo è stato registrato a seguito di un residuale finanziamento riconosciuto all'Ufficio dal competente dicastero finanziario dopo oltre due mesi dalla chiusura dell'esercizio finanziario. La misura effettivamente acquisita in conto esercizio 2012 ammonta a complessivi 8,8 milioni di euro e rappresenta il 38% circa del totale delle entrate accertate nell'anno dall'Autorità.

Ulteriore fonte di finanziamento è rappresentata dai proventi derivanti dalle sanzioni pecuniarie comminate dall'Ufficio, che hanno fatto affluire in bilancio 1,9 milioni di euro, rispetto a 1,5 milioni di euro del 2011, facendo così registrare un incremento di oltre il 26%.

In proposito va considerato che nel 2012 le sanzioni versate dai debitori direttamente alla Tesoreria dello Stato, e quindi acquisite al bilancio erariale, sono state pari a 3,7 milioni di euro. Di queste, il Garante -facendosi carico della relativa istruttoria- ha ottenuto dal competente ministero la riassegnazione, nella misura del 50% stabilita per legge.

Va aggiunto che è a carico del Garante l'istruttoria per la riscossione coattiva delle sanzioni, mediante iscrizione a ruolo delle somme non versate spontaneamente dai soggetti sanzionati, tramite l'agente della riscossione Equitalia.

Per quanto attiene alla spesa sostenuta, l'attività amministrativa si è svolta prestando particolare cura al rispetto dei vincoli e degli indirizzi di contenimento della spesa già previsti da disposizioni legislative e dalle misure di *spending review* rese operative nel 2012.

La spesa complessiva nel 2012 è stata di 19,7 milioni di euro, in significativa contrazione rispetto alle somme stanziate in sede di previsione.

La spesa corrente si è contratta rispetto alle stime iniziali di circa il 13% mentre per la spesa in conto capitale, riguardante i beni ad utilità pluriennale, la riduzione ha inciso per oltre il 50%; ciò è stato possibile grazie ad una specifica scelta gestionale, favorita anche dalle misure adottate dal legislatore, che hanno reso indispensabile realizzare nell'anno delle economie di spesa.

Quanto alle auto di servizio, resta in uso soltanto il veicolo assegnato dal Ministero delle infrastrutture e destinato -in via esclusiva- al Presidente, in linea con le recenti disposizioni in materia.

Non vi sono state spese per consulenze ed è proseguita l'applicazione delle misure di riduzione dei compensi degli organi collegiali. Ulteriori attività di razionalizzazione gestionale hanno consentito un contenimento della spesa rispetto alle previsioni iniziali.

Per quanto attiene agli emolumenti corrisposti al personale si è data applicazione alla sentenza con cui, nella seconda parte dell'anno, la Corte costituzionale ha dichiarato, tra l'altro, l'incostituzionalità delle disposizioni che imponevano una riduzione delle retribuzioni di importo superiore ad euro 90.000 annui.

La parte più significativa della spesa resta comunque quella avente carattere fisso e continuativo, per la quale non sono praticabili ulteriori margini di intervento rispetto a quelli già adottati dall'Ufficio.

La rimanente parte della spesa, relativa al funzionamento dell'Ufficio, è ricondotta entro i limiti previsti dalle disposizioni finanziarie di contenimento della spesa pubblica applicabili all'Autorità.

La spesa per l'acquisizione di beni durevoli, aventi un'utilità pluriennale, ha registrato una significativa riduzione rispetto alle previsioni iniziali evidenziando una importante contrazione anche rispetto alle analoghe tipologie di oneri del precedente esercizio, a conferma di un generalizzato criterio di contenimento dei costi, che non ha però comportato rallentamenti dell'attività amministrativa.

La tabella allegata alla presente Relazione (cfr. *infra* par. 24., tab. 21.) riassume e mette a confronto i valori finanziari che hanno interessato la gestione dell'Autorità nel 2012 e nel 2011 evidenziando anche gli scostamenti registrati tra i due periodi.

In particolare, la tabella elenca le fonti di finanziamento complessive evidenziando gli importi posti a carico del bilancio dello Stato.

Per quanto riguarda la spesa, l'onere complessivo sostenuto dall'Ufficio per lo svolgimento delle attività istituzionali trova separata evidenza tra la spesa connessa al funzionamento, comprensiva degli oneri per gli organi e per il personale, e quella per investimento e per rimborsi, nonché per restituzioni in favore del bilancio dello Stato.

23.2. L'ATTIVITÀ CONTRATTUALE E LA GESTIONE ECONOMALE

L'attività contrattuale dell'Autorità, nel 2012, è stata improntata a conseguire, coerentemente con gli indirizzi di carattere generale, i migliori risultati in termini di efficienza e di risparmio.

In particolare, si è tentato costantemente, allo spirare dei contratti in corso, da un lato, di unificarli, accorpando le varie esigenze ad essi relativi e, dall'altro, di prolungare i tempi medi dei contratti stessi, in conformità ai princìpi dettati dal Codice dei contratti pubblici.

È stato fatto costante riferimento alle convenzioni Consip ed è stato utilizzato, ogni qual volta ciò sia risultato possibile, il ricorso al Mercato elettronico della p.a. (Mepa), tramite richiesta di offerta o acquisto diretto, con buoni risultati in termini di efficienza operativa e di risparmio.

In particolare, sono state utilizzate le convenzioni Consip per il completamento della fornitura di fotocopiatrici, per gli interventi di manutenzione del centralino telefonico e per i servizi di *facility management* (pulizia, *reception*, minuta manutenzione della sede).

Per quanto riguarda il Mepa, nel periodo in considerazione, si è ricorsi allo strumento della richiesta di offerta (RdO) nel 61% del totale delle procedure di gara ed agli affidamenti diretti al miglior offerente nel 19% del totale degli affidamenti.

Anche nell'anno in considerazione è stata svolta una procedura aperta per la selezione del servizio di assistenza sanitaria a favore dei dipendenti, che però -anche in questa occasione- è andata deserta, rendendo necessario procedere con successiva procedura negoziata (riguardo all'esistenza di "*diffuse criticità*" concernenti l'affidamento dei servizi assicurativi si rinvia alla consultazione pubblica effettuata nel corso dell'anno 2012 dall'Autorità per la vigilanza sui contratti pubblici di lavori, v. al riguardo www.avcp.it).

In ragione dell'urgenza, della maggiore economicità della procedura e, talvolta, in relazione al bene/servizio richiesto, si è in alcuni casi ricorsi al cottimo fiduciario, con buoni risultati in termini di risparmio rispetto agli importi stabiliti a base d'asta.

Nel corso dell'anno sono stati poi eseguiti alcuni affidamenti diretti *ex* art. 57, comma 2, lett. *b)*, del Codice dei contratti pubblici (fornitore unico), in particolare con riferimento ad alcuni prodotti informatici e di agenzie di informazione.

Sono stati infine effettuati, mediante procedura negoziata, numerosi atti di cd. "micro-contrattualistica", in relazione ad esigenze di importi esigui.

Per quanto riguarda l'attività di carattere economale, l'anno in considerazione è stato contrassegnato da un'importante azione di redistribuzione degli spazi con connessa razionalizzazione dell'allocazione degli uffici all'interno dell'immobile adibito a sede dell'Autorità e la retrocessione di alcune porzioni immobiliari alla proprietà. Ciò ha reso necessaria l'effettuazione di alcuni lavori di sistemazione, soprattutto di carattere impiantistico.

Sono stati altresì effettuati taluni interventi di manutenzione ordinaria, nonché l'acquisto di alcuni arredi in sostituzione di quelli maggiormente obsoleti e non più rispondenti ai requisiti di sicurezza.

Inoltre, è stato dismesso un magazzino, rivelatosi nel corso degli anni sovradimensionato rispetto alle esigenze del Garante, a favore dell'utilizzo di un locale molto più ridotto con un conseguente, sensibile risparmio in termini di canoni di locazione.

Il magazzino rilasciato reca una pendenza in ordine al pagamento di alcuni oneri di occupazione, nei confronti dell'amministrazione pubblica a suo tempo proprietaria, relativamente agli anni 1998-2005, ed al fine di giungere ad una soluzione condivisa è stata avviata un'ipotesi transattiva con la proprietà, che ha ricevuto un preventivo assenso di massima da parte dell'Avvocatura dello Stato.

23.3. LE NOVITÀ LEGISLATIVE E REGOLAMENTARI E L'ORGANIZZAZIONE DELL'UFFICIO

Nel 2012 è proseguita la rigorosa attuazione delle misure di contenimento della spesa pubblica previste dal d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122. Anche nel 2012, infatti, non ci sono state spese per consulenze, e quanto alle auto di servizio, l'Autorità continua a disporre esclusivamente della vettura assegnata dal Ministero delle infrastrutture e trasporti per le esigenze di mobilità del Presidente dell'Autorità.

Nella seconda parte del 2012, in coincidenza con l'insediamento del nuovo Collegio, si è avviata una riflessione sul complessivo assetto funzionale e organizzativo dell'Autorità per delineare possibili linee di sviluppo organizzativo al fine di valorizzare le risorse a disposizione

dell'Autorità e migliorare le capacità di risposta ai cittadini nonché di fornire, alla luce dei previsti mutamenti del quadro normativo comunitario, contributi utili al dibattito, ormai aperto a livello europeo, su come assicurare un livello elevato e uniforme di protezione dei dati personali rispondendo alle sfide della globalizzazione e dell'evoluzione tecnologica e ai rischi e alle potenzialità in esse insiti.

La riflessione proseguirà nel 2013; nelle more sono stati rinnovati gli incarichi dirigenziali e, nel quadro di un processo di razionalizzazione dei compiti svolti dalle attuali unità organizzative, sono stati apportati i primi correttivi, istituendo l'unità organizzativa temporanea "Organizzazione e controllo di gestione", a supporto delle scelte organizzative, potenziando ulteriormente il flusso di dati sull'attività dell'Ufficio, in vista dell'attuazione del primo modulo di un sistema informativo direzionale dell'Autorità avente anche finalità di controllo di gestione.

Pur nel contesto di una sensibile riduzione dello stanziamento a disposizione dell'Autorità, nel 2012 si è conclusa la procedura di mobilità volontaria ai sensi dell'art. 30 del d.lgs. n. 165/2001, riservata al personale in posizione di fuori ruolo presso l'Ufficio da almeno un anno, indetta nel dicembre del 2011 al fine di acquisire stabilmente all'organico dell'Autorità personale in possesso di specifiche professionalità e di requisiti adeguati e comprovati.

Per far fronte alla persistente sproporzione tra i compiti istituzionali demandati al Garante dal Codice e dalla normativa comunitaria e l'organico a disposizione, agli inizi del 2013 è stata inoltre assunta la decisione di indire due procedure di mobilità volontaria esterna, ai sensi del medesimo art. 30 del citato d.lgs. n. 165/2001, riservate ai dipendenti delle pubbliche amministrazioni con rapporto di lavoro a tempo indeterminato, rispettivamente per n. 3 funzionari con profilo informatico-tecnologico e per n. 2 funzionari con profilo giuridico.

Servizio segreteria del Collegio

Il servizio di segreteria del Collegio ha curato anche quest'anno gli adempimenti necessari allo svolgimento delle attività di tale organo (predisposizione e distribuzione della documentazione necessaria per le riunioni del Collegio; conservazione dei verbali e degli originali delle deliberazioni adottate e del materiale utile per le pubblicazione in Gazzetta Ufficiale).

Inoltre il servizio, in stretto raccordo con le diverse articolazioni dell'Ufficio, ha provveduto all'attento controllo dei testi deliberati e destinati -tramite la redazione web- alla pubblicazione sul sito istituzionale dell'Autorità.

Nel 2012, conformemente a quanto disposto dall'art. 15 del Regolamento n.1/2000 e nel rispetto del codice dell'amministrazione digitale, l'Autorità ha adottato modalità di trasmissione elettronica dei documenti predisposti per l'esame o l'approvazione del Collegio, che consentono maggiore celerità ed efficienza nonché la progressiva sostituzione del mezzo cartaceo con quello elettronico, con risparmio di costi e tempo nonché recupero di spazio.

Nella stessa prospettiva si segnala la piena fruibilità, nella intranet, dei testi dei provvedimenti adottati dal Collegio, che dopo l'introduzione nel 2011 del registro delle deliberazioni collegiali di cui si è riferito nella Relazione 2011 (p. 238), si avvale anche della funzionalità di ricerca e dei miglioramenti tecnici connessi all'avvio del nuovo sito del Garante, di cui si riferisce più diffusamente nel paragrafo 23.5..

23.4. IL PERSONALE E I COLLABORATORI ESTERNI

Nel 2012, a conclusione della procedura di mobilità volontaria riservata al personale in posizione di fuori ruolo presso l'Ufficio, sono stati immessi nel ruolo organico tre funzionari e un impiegato operativo.

Sono stati rinnovati alcuni contratti a tempo determinato, sulla base di un accordo negoziale sottoscritto con le rappresentanze sindacali del personale (ai sensi dell'art. 5, comma 4-*bis*, del d.lgs. n. 368/2001), con il quale si è convenuto di prevedere la possibilità di un rinnovo quadriennale dei contratti di lavoro in scadenza.

Per evitare discontinuità nelle attività istituzionali e nell'attuazione dei programmi di lavoro cui il personale a contratto risulta attualmente assegnato, con pregiudizievoli conseguenze sui livelli di tutela dei cittadini attualmente assicurati dall'Autorità, con successivo accordo negoziale, sottoscritto ai sensi del comma 3 del medesimo art. 5 del d.lgs. n. 368/2001, si è convenuto, altresì, di prevedere un termine ridotto a venti o trenta giorni in luogo di quello ordinario di sessanta o novanta giorni a seconda che il primo contratto abbia una durata inferiore o superiore a sei mesi, per il rinnovo del contratto.

Nel periodo considerato si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2012 l'Ufficio poteva contare su un organico, a diverso titolo, di 108 unità, di cui 104 in servizio, al quale va aggiunto un contingente di personale a contratto di 18 unità.

Dai suddetti dati si evidenzia che nell'anno considerato si è verificato un contenuto incremento del personale in servizio rispetto all'anno precedente e, in particolare di quello di ruolo, che rappresenta poco più dell'80% del totale.

Nel periodo considerato, l'Autorità si è avvalsa delle figure professionali previste dalla vigente normativa in materia di sicurezza e incolumità dei lavoratori nei luoghi di lavoro (medico competente e responsabile del servizi di prevenzione e sicurezza).

Presso l'Autorità opera il servizio di controllo interno presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettivamente, della Ragioneria generale dello Stato e della Presidenza del Consiglio dei ministri.

23.5. IL SETTORE INFORMATICO E TECNOLOGICO

Sviluppo del sistema informativo e dei servizi ICT

Nel 2012 è proseguita l'attività di sviluppo del sistema informativo, con tutti gli strumenti di innovazione previsti dal Codice dell'amministrazione digitale (Cad), ed un forte impulso verso i processi volti alla cd. smaterializzazione dei flussi documentali delle attività amministrative e della cooperazione interna.

In tale contesto, è stato attuato l'accordo di collaborazione con il Ministero degli affari esteri per il riuso della piattaforma "documentale @doc" che, dal primo semestre 2013, permetterà di smaterializzare i flussi documentali relativi ad alcuni procedimenti amministrativi.

Nell'ottobre 2012 è stato messo in rete il nuovo sito web istituzionale, basato su strumenti di gestione dei contenuti e su sistemi di *database open source*, che consentono una più agevole gestione delle informazioni -offrendo nel contempo un'interfaccia più moderna- funzioni di ricerca avanzate basate sul paradigma del web semantico e prestazioni più elevate in termini di velocità di risposta.

È stata sviluppata nel 2012 una procedura basata su modulistica elettronica in formato Pdf per la notifica dei *data breach* al Garante, disponibile sul sito per l'utilizzo da parte dei fornitori di servizi di comunicazione elettronica che abbiano subito una violazione dei dati personali.

In parallelo è stata sviluppata in ambiente intranet una sezione per la gestione della documentazione relativa alle adunanze, pervenendo alla totale dematerializzazione della stessa, dall'ordine del giorno all'approvazione delle delibere (v. *supra* par. 23.3.). I fascicoli informatici vengono assegnati ai relatori e messi a disposizione del Presidente e dei componenti il Collegio consentendo così una maggiore efficienza nell'esame degli atti, anche grazie all'utilizzo di terminali mobili di tipo *tablet*.

Sempre in ambito intranet è stata sviluppata l'area relativa alla formazione del personale, dalle comunicazioni relative agli eventi formativi, ai calendari, alla gestione del materiale didattico.

È stata effettuata la migrazione alla nuova versione del sistema di gestione informatica del protocollo, con l'attivazione di *web services* che consentono l'interfacciamento del sistema con altri moduli del sistema informativo del Garante. Le nuove funzionalità comprendono un sistema di autenticazione *Single sign on* (Sso), che consente la protocollazione decentrata e l'interfacciamento con i sistemi di posta elettronica certificata (Pec).

L'accesso condiviso di tipo Sso è stato configurato anche per i servizi bibliotecari dell'Ufficio, incrementando altresì il numero delle banche dati disponibili.

A livello di infrastruttura IT, è stata effettuata la migrazione del dominio *Active Directory*, e della maggior parte dei *server* utilizzati per l'erogazione dei servizi informatici interni sui sistemi *Windows Server* 2008R2. È stato inoltre adottato, per il monitoraggio dei *server*, delle postazioni di lavoro, degli apparati di rete e di altri dispositivi IT, il sistema *open source Nagios* che consente la precoce scoperta di situazioni pregiudizievoli per la continuità di erogazione dei servizi e per la sicurezza dei dati. È stata infine introdotta una nuova procedura per il pagamento elettronico via web, mediante carta di credito, dei diritti di segreteria relativi alla notificazione telematica dei trattamenti di dati personali o alle istanze di verifica preliminare.

È stata realizzata una nuova infrastruttura di rete *wi-fi* a copertura dell'intera sede dell'Ufficio e a supporto delle applicazioni di tipo mobile nonchè migliorata la rete locale (LAN).

Impegno per la sicurezza informatica dell'Ufficio

Anche nel 2012 nessun incidente informatico di rilievo è occorso nel dominio dell'Ufficio e, in particolare, nessun evento relativo alla sicurezza ha prodotto danni o disservizi. Relativamente ai virus informatici, la cui diffusione è andata incontro a notevole espansione,

i controlli sui trasferimenti da supporti o tramite connessioni di rete e posta elettronica hanno consentito di neutralizzare i contenuti nocivi occasionalmente rilevati. Non si sono verificate perdite di dati sottoposti a *backup* e, alle occasionali indisponibilità o cancellazione accidentali di *file* o di documenti, è stato possibile sempre porre rimedio con le ordinarie procedure o con i servizi di assistenza.

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento risorse tecnologiche ha fornito nel 2012 supporto consultivo alle unità dell'area giuridica dell'Ufficio, formulando analisi tecniche per le fasi istruttorie dei diversi procedimenti dell'Autorità, note informative e relazioni su diverse tematiche emerse nello svolgimento delle attività istituzionali. Ha inoltre partecipato a incontri e riunioni di lavoro, preliminari a interventi dell'Autorità in convegni o su organi di stampa, nel corso dei quali sono stati affrontati i profili tecnologici di temi di pubblico interesse. Tra i principali interventi svolti si evidenzia, nell'ambito delle telecomunicazioni e di internet, la collaborazione per la stesura del provvedimento sul trattamento dei dati personali, anche di natura sensibile, all'interno di *blog* o siti web dedicati a temi sanitari [doc. web n. 1870212]. Sono inoltre proseguite le attività istruttorie per l'autorizzazione al trattamento di dati aggregati di traffico telefonico, eventualmente "arricchiti" mediante l'impiego di dati territoriali di natura statistica o provenienti da basi di dati georeferenziate (provv. 15 marzo 2012 [doc. web n. 1903026]), per finalità di profilazione a scopo di *marketing*. Infine è stato fornito un inquadramento tecnologico propedeutico alla definizione dei provvedimenti posti in consultazione pubblica in tema di violazione di dati personali (*data breach*) [doc. web n. 1915485] e sull'utilizzo dei *cookie* per finalità di tracciamento della navigazione web degli utenti [doc. web n. 2139697].

Nel settore delle realtà economiche e produttive la collaborazione ha riguardato le tecnologie biometriche, in particolare, il provvedimento di verifica preliminare sull'impiego di tecniche grafometriche di sottoscrizione o di riconoscimento [doc. web n. 2311886]. Inoltre, è stato fornito supporto nell'interazione con Abi e con gli istituti di credito relativamente agli adempimenti tecnici riguardanti le prescrizioni contenute nel provvedimento "tracciabilità banche" [doc. web n. 1813953].

In materia di libertà pubbliche e sanità si segnala la collaborazione nell'applicazione del cosiddetto *Privacy Impact Assessment* (PIA), ossia delle valutazioni che il titolare è tenuto a

svolgere in caso di trattamenti che coinvolgano dati sanitari, in particolare per l'utilizzo di tecnologie a radiofrequenza (*Rfid - Radio frequency identification*) con impianto sottocutaneo, nell'ambito di una verifica preliminare presentata da un costruttore di apparati per defibrillazione [doc. web n. 2276103]. Si cita, inoltre, il supporto reso per l'analisi e l'elaborazione di provvedimenti relativi ai decreti ministeriali di istituzione di nuovi flussi informativi nell'ambito del Nuovo Sistema Informativo Sanitario (NSIS) [doc. web nn. 1900890, 1907937, 1893476, 1892560]; la consulenza nell'ambito del parere sul provvedimento del Direttore dell'Agenzia delle entrate inerente la comunicazione integrativa all'archivio dei rapporti finanziari [doc. web n. 1886775] e il parere reso sul sistema delle anagrafi regionali degli studenti [doc. web n. 2304850].

Nell'ambito delle relazioni istituzionali, molteplici sono stati i pareri su atti di natura regolamentare. Tra questi, si citano: il parere relativo alla Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze riguardante l'accesso da parte delle forze di polizia, tramite il Ced del Dipartimento della pubblica sicurezza, al Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf) [doc. web n. 1915461]; quello sullo schema di decreto del Presidente del Consiglio dei Ministri in materia di consegna, da parte delle aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento *online* delle prestazioni erogate [doc. web n. 2223206]; lo schema di provvedimento del Direttore generale per gli italiani all'estero in materia di passaporto elettronico [doc. web n. 2222980]; lo schema di regolamento del Ministro dell'economia e delle finanze concernente l'uso degli strumenti informatici e telematici nell'ambito del processo tributario in attuazione delle disposizioni contenute nell'art. 39, comma 8, lett. *d*), del d.l. 6 luglio 2011, convertito, con modificazioni, dalla l. 15 luglio 2011, n. 111 [doc. web n. 2185215]; lo schema di decreto del Ministro dell'interno riguardante modifiche al d.m. 11 dicembre 2000, recante "Disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive" [doc. web n. 2099252]; lo schema di decreto dirigenziale *ex* art. 39 del d.P.R. n. 313/2002, sul Sistema informativo del Casellario (SiC) [doc. web n. 2091248]; lo schema di decreto del Ministro

dell'interno sulle regole tecniche per il permesso di soggiorno elettronico [doc. web n. 1908393]; lo schema di decreto del Ministero dell'economia e delle finanze relativo al sistema Sirfe - antifrode banconote e monete; il parere sul servizio telematico revisori legali della Ragioneria generale dello Stato.

Contributi all'attività ispettiva

Nel 2012 è altresì proficuamente continuata la collaborazione relativa ad importanti attività ispettive, con la realizzazione di accessi a banche dati, l'analisi e lo studio dei materiali acquisiti, la stesura di rapporti e la formulazione di misure e accorgimenti di natura tecnologica.

Tra le attività più significative in questo ambito si segnalano: la campagna esplorativa sui servizi di *mobile payment,* pagamenti effettuabili sia con addebito sul conto telefonico per l'acquisto di beni digitali, sia per la "virtualizzazione" delle carte di credito all'interno delle Sim dei gestori di telefonia mobile per l'acquisto di beni e servizi in tecnologia NFC; le ispezioni propedeutiche all'adozione di un provvedimento generale sulle cd. "chiamate mute" nel *telemarketing*; le attività ispettive in ambito sanitario; gli accertamenti sui *data breach*, anche in relazione alle recenti modifiche apportate agli artt. 32 e 32-*bis* del Codice; l'attività ispettiva relativa alla tenuta dei registri di protocollo informatico; l'ispezione Schengen presso la divisione Sirene per l'applicazione dell'art. 95 CAAS; ed infine ulteriori attività ispettive, tra l'altro, presso l'Agenzia delle entrate.

Contributi all'attività internazionale

Profili di interesse tecnologico nell'attività internazionale dell'Autorità sono emersi nell'ambito sia dei gruppi di esperti nominati dalla Commissione europea su temi specifici, sia delle attività istituzionali del Gruppo Art. 29, con studio di documenti e produzione di rapporti. Si segnalano in particolare, la partecipazione ai lavori del *Technology Subgroup* del Gruppo Art. 29, che affronta le tematiche di attualità nell'area ICT in materia di protezione dei dati personali. Degno di nota, in tal senso, è il ruolo di *rapporteur* svolto dal Garante, insieme ad altre autorità di protezioni dati, per l'elaborazione del parere reso dal Gruppo in tema di *cloud computing*. Il Dipartimento ha poi rappresentato l'Autorità nel Gruppo di Berlino per le telecomunicazioni, partecipando ai due *meeting* svoltisi nel 2012 e contribuendo alla redazione di documenti ufficiali del Gruppo, con specifico riferimento alle modalità tecniche per la realizzazione del cosiddetto diritto all'oblio su internet e negli archivi *online*.

Significativo è stato altresì l'impegno svolto dal personale del Dipartimento per presentare relazioni a seminari, *workshop* e convegni sugli aspetti tecnologici della protezione dei dati personali. Tra questi, gli interventi al convegno "*Cloud* e diritto" presso l'Università Bocconi di Milano (17 maggio 2012), sul *cloud computing* nell'ambito del Forum Pa 2012 (18 maggio 2012) e al convegno "Il *cloud computing* nel sistema finanziario: *standard*, regolamentazione e controlli" della Banca d'Italia (28 settembre 2012) nonché la partecipazione alla 6ª edizione della ISSA Security Conference 2012 (18 ottobre 2012).

Il Dipartimento ha inoltre costantemente offerto supporto, in collaborazione con l'Urp, nelle risposte a quesiti e richieste di chiarimento relative a normativa e provvedimenti del Garante in tema di sistemi ICT.

24. I DATI STATISTICI (*)

1. Sintesi delle principali attività dell'Autorità

SINTESI DELLE PRINCIPALI ATTIVITÀ DELL'AUTORITÀ	
Numero complessivo dei provvedimenti collegiali adottati	440
Ricorsi decisi (art. 145 del Codice)	233
Pareri a Presidenza del Consiglio dei ministri e ministeri (artt. 54 e 154 del Codice)	23
Notificazioni pervenute nell'anno 2012	1.053
Notificazioni pervenute dal 2004 al 31 dicembre 2012	21.027
Violazioni amministrative contestate	578
Sanzioni applicate con ordinanza di ingiunzione	118
Violazioni penali segnalate all'autorità giudiziaria	56
Riscontri a segnalazioni e reclami	4.183
Risposte a quesiti	326
Ricorsi (trattati) *ex* art. 152 del Codice	78
Opposizioni (trattate) a provvedimenti del Garante	73
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	395
Altre richieste ai sensi dell'art. 157 del Codice non effettuate direttamente presso i titolari	142
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	10
Provvedimenti su verifiche preliminari per trattamenti che presentano rischi specifici	13
Comunicazioni al Garante su flussi di dati tra p.a. o in temi di ricerca	9
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	5
Risposte ad atti di sindacato ispettivo e di controllo	6
Leggi regionali esaminate (di cui con rilievi ai fini dell'impugnazione *ex* art. 127 della Costituzione)	18 (1)
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	30
Riunioni autorità comuni di controllo (Europol, Schengen, Dogane, Eurodac), del *Wppj* e del *Future of Supervision Group*	23
Riunioni presso il CoE, OCSE e altri organismi internazionali	9
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	18

2. Altre attività dell'Autorità

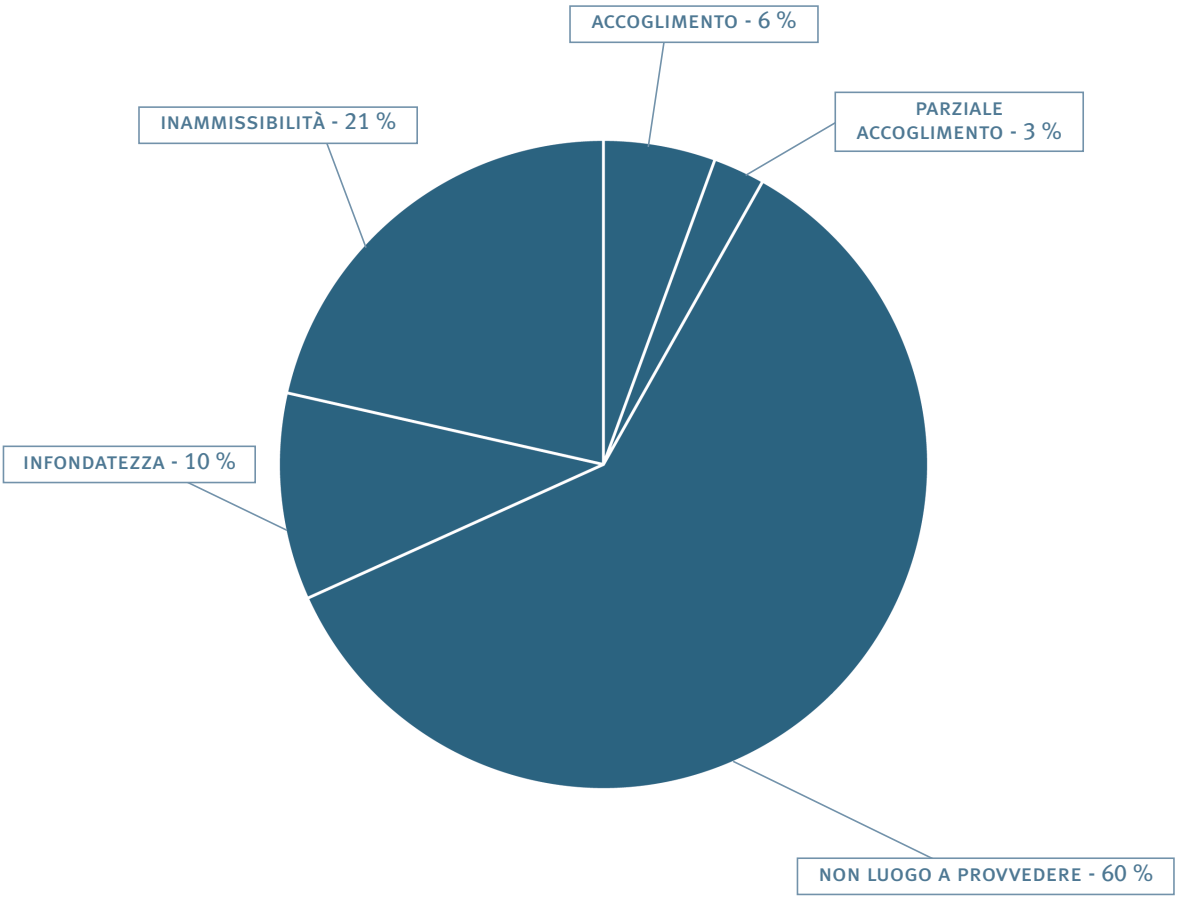
ALTRE ATTIVITÀ DELL'AUTORITÀ	
Comunicati stampa	29
Newsletter	13
Dvd (archivio digitale su normativa italiana e attività del Garante)	1
Cd (archivio digitale su normativa europea)	1
Vademecum	2
Prodotti editoriali	2
Video divulgativi	1
Conferenze internazionali (1)	2

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2012. Singole note indicano altri periodi o situazioni e casi specifici. I dati delle tabelle 9, 10, 11 si riferiscono ai fascicoli istituiti presso l'Ufficio

(1) Una delle due conferenze è stata organizzata congiuntamente dal Servizio relazioni internazionali e dal Servizio relazioni con i mezzi di informazione

3. Tipologia delle decisioni su ricorsi (tabella e grafico)

DECISIONI SU RICORSI	
TIPI DI DECISIONE (1)	NUMERO RICORSI
Accoglimento	13
Parziale accoglimento	6
Non luogo a provvedere (2)	140
Infondatezza	24
Inammissibilità	50
Totale	**233**

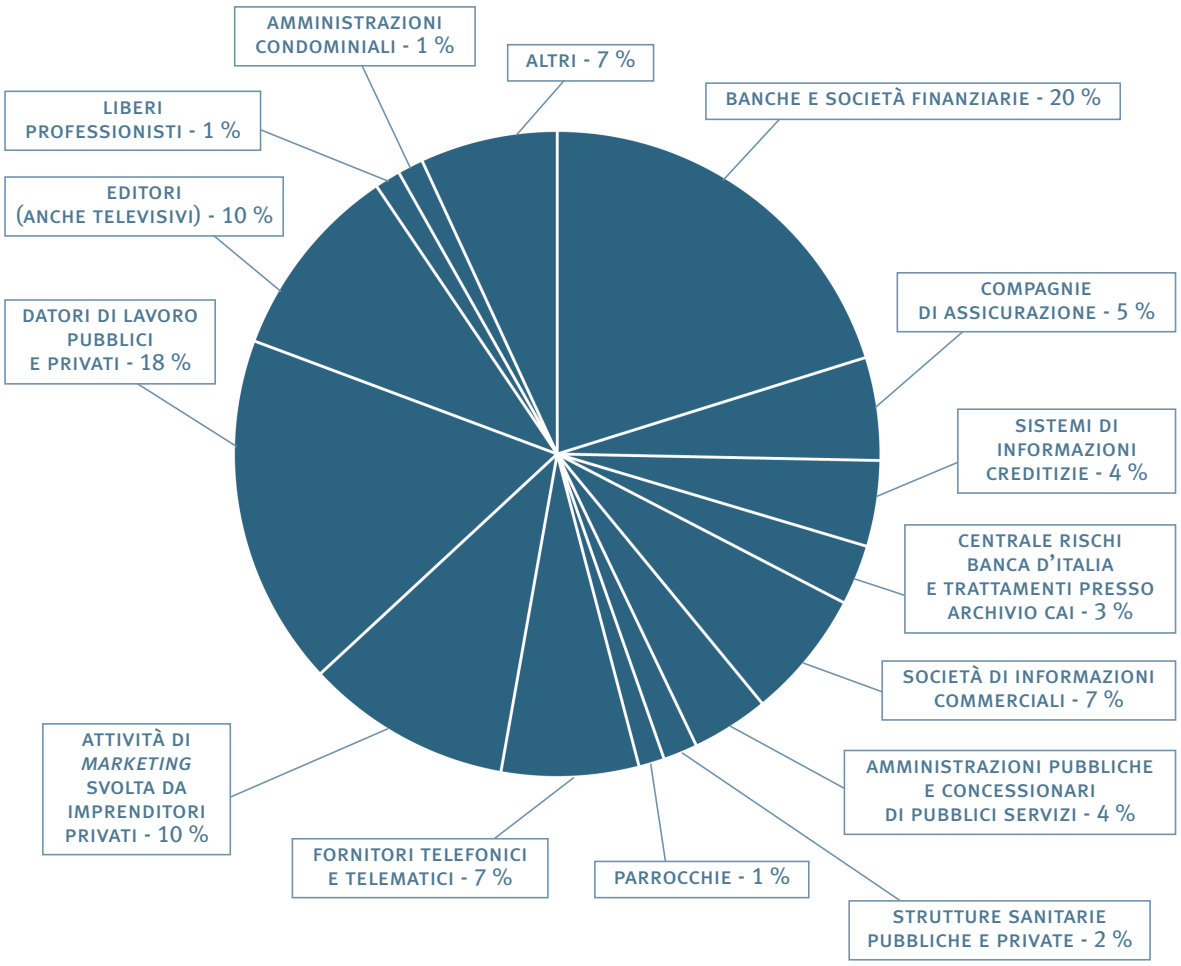


(1) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole"

(2) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

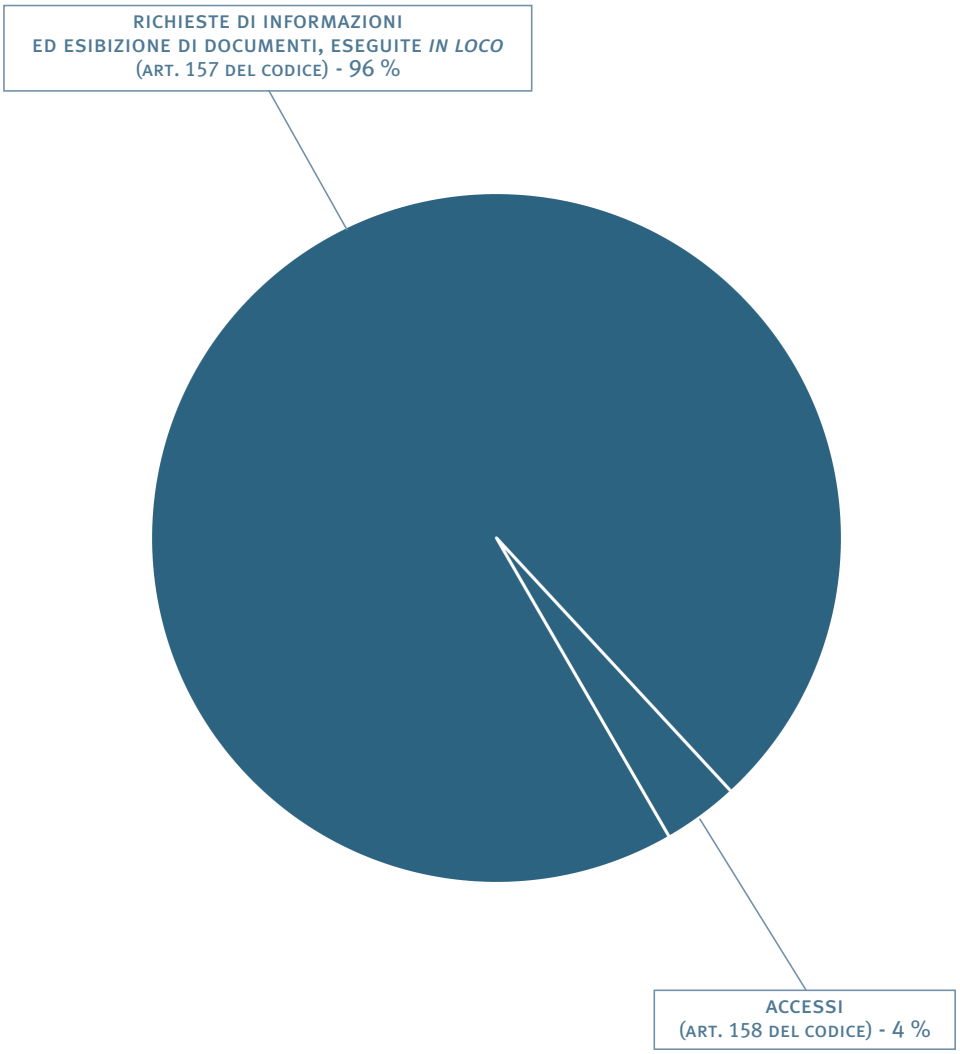
4. Suddivisione dei ricorsi in relazione alla categoria di titolari del trattamento (tabella e grafico)

CATEGORIA DI TITOLARI	NUMERO RICORSI
Banche e società finanziarie	47
Compagnie di assicurazione	12
Sistemi di informazioni creditizie	10
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	7
Società di informazioni commerciali	15
Amministrazioni pubbliche e concessionari di pubblici servizi	9
Strutture sanitarie pubbliche e private	4
Parrocchie	3
Fornitori telefonici e telematici	16
Attività di *marketing* svolta da imprenditori privati	24
Datori di lavoro pubblici e privati	41
Editori (anche televisivi)	23
Liberi professionisti	3
Amministrazioni condominiali	3
Altri	16
Totale	233



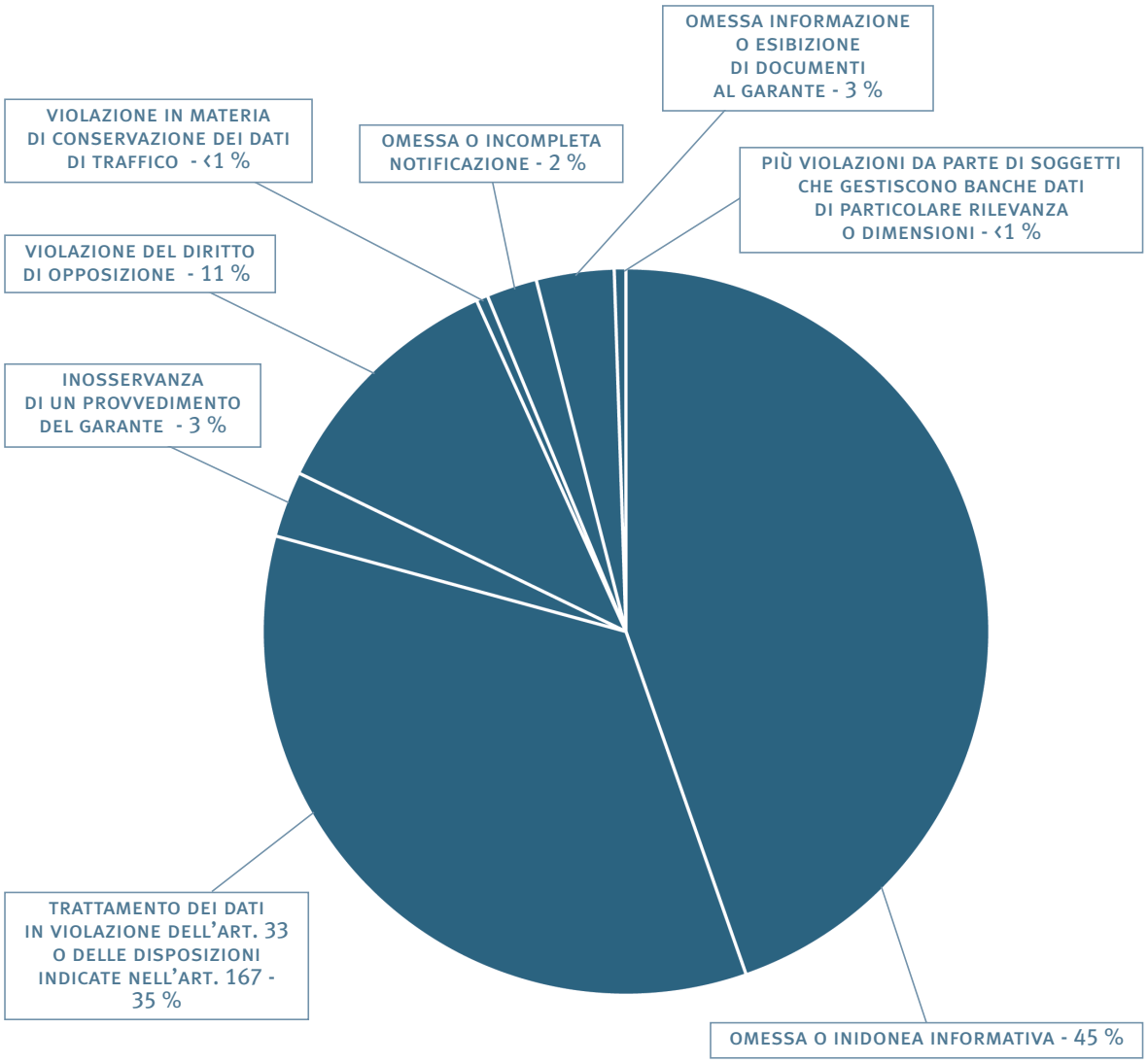
5. Accertamenti e controlli eseguiti (tabella e grafico)

ACCERTAMENTI E CONTROLLI ESEGUITI DIRETTAMENTE PRESSO TITOLARI DEL TRATTAMENTO	
Richieste di informazioni ed esibizione di documenti, eseguite *in loco* (art. 157 del Codice)	381
Accessi (art. 158 del Codice)	14
Totale	**395**



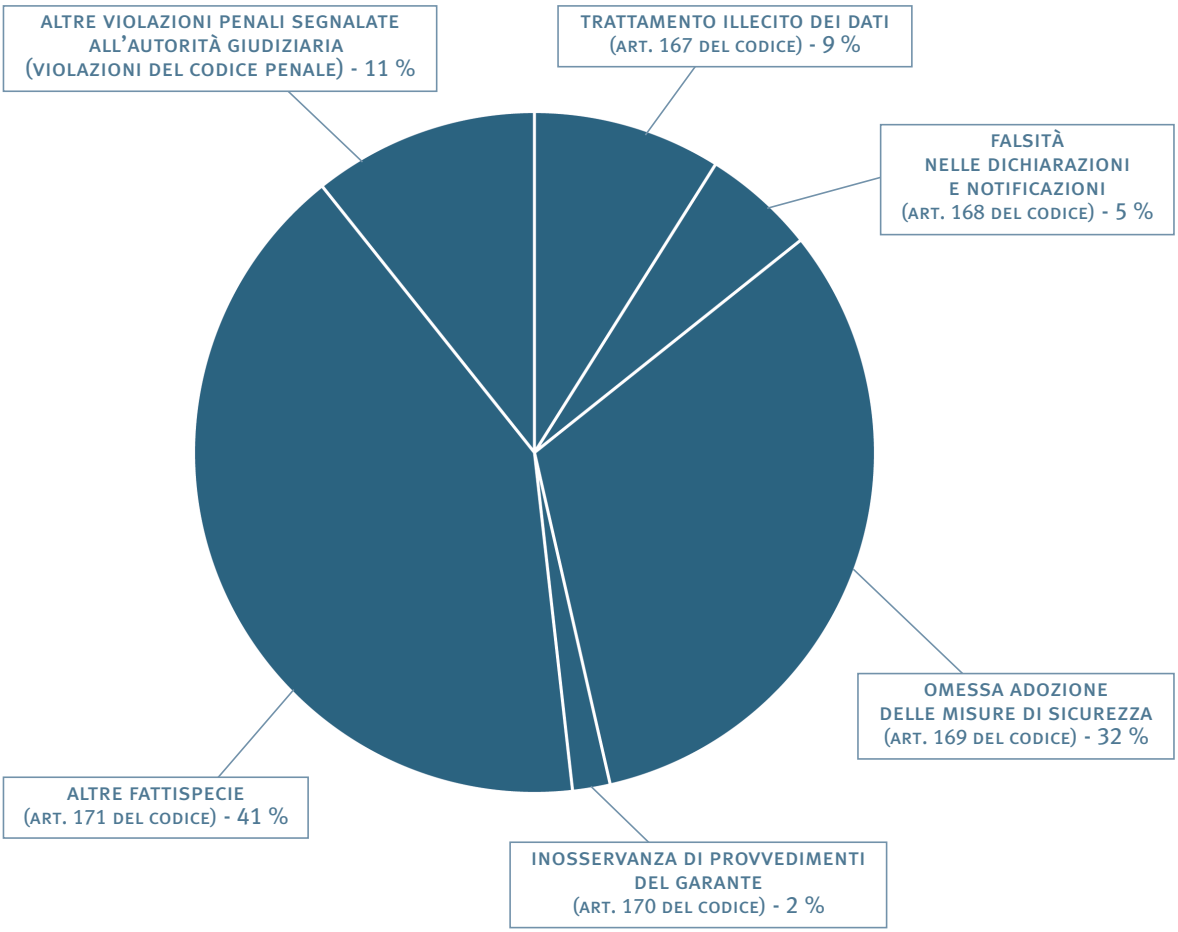
6. Violazioni amministrative contestate (tabella e grafico)

VIOLAZIONI AMMINISTRATIVE CONTESTATE	
Omessa o inidonea informativa (art. 161 del Codice)	258
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	200
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	17
Violazione del diritto di opposizione (art. 162, comma 2-*quater*, del Codice)	64
Violazione in materia di conservazione dei dati di traffico (art. 162-*bis*, del Codice)	3
Omessa o incompleta notificazione (art. 163 del Codice)	13
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	20
Più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	3
Totale	578



7. Violazioni penali segnalate all'autorità giudiziaria (tabella e grafico)

VIOLAZIONI PENALI SEGNALATE ALL'AUTORITÀ GIUDIZIARIA	
	SEGNALAZIONI
Trattamento illecito dei dati (art. 167 del Codice)	5
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	3
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	18
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	1
Altre fattispecie (art. 171 del Codice)	23
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del codice penale)	6
Totale	56



8. Pagamenti derivanti dall'attività sanzionatoria

PAGAMENTI DERIVANTI DALL'ATTIVITÀ SANZIONATORIA	
Somme versate a titolo di oblazione in via breve	2.928.267
Somme versate in conseguenza di ordinanze ingiunzione	780.950
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	60.000
Totale	**3.769.217**

9. Pareri (*ex* art. 154, comma 4, del Codice)

PARERI (*EX* ART. 154, COMMA 4, DEL CODICE)	
TEMI	RISCONTRI RESI NELL'ANNO (1)
Attività di polizia, sicurezza nazionale e governo del territorio	3
Giustizia	2
Informatizzazione e banche dati della p.a.	6
Formazione	1
Tutela della salute e attività sanitaria	1
Attività produttive e professioni	1
Esercizio dei diritti	2
Solidarietà sociale	3
Documenti elettronici	2
Totale	**21**

10. Quesiti

QUESITI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	**320**	**326**

11. Segnalazioni e reclami

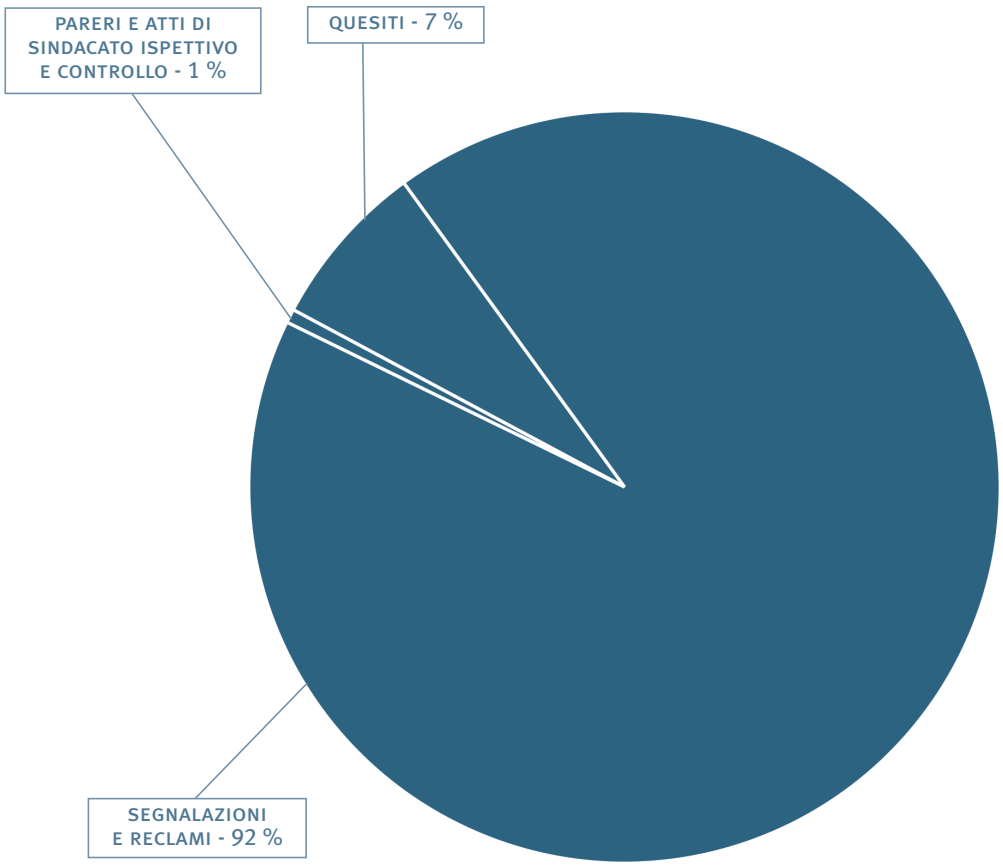
SEGNALAZIONI E RECLAMI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	**4.592**	**4.183**
TEMI PRINCIPALI		
Assicurazioni	81	81
Associazioni	41	41
Centrali rischi	134	134
Concessionari pubblici servizi	121	121
Condominio	26	26
Credito	291	291
Enti locali	49	49
Giornalismo e libertà d'espressione	200	186
Imprese	135	135
Informazioni commerciali	9	9
Istruzione	19	19
Lavoro	288	224
Marketing	21	21
Recupero crediti	138	138
Sanità e servizi di assistenza sociale	23	47
Telefonia	1.982	1.844
Tributi	5	14
Videosorveglianza	172	181

(1) Inerenti anche ad affari pervenuti anteriormente al 2012

12. Atti di sindacato ispettivo e controllo

ATTI DI SINDACATO ISPETTIVO E CONTROLLO	
TEMI	NUMERO
Trattamento di dati personali nel settore bancario	1
Servizio *"Street view"* da parte di Google	1
Marketing telefonico, registro pubblico delle opposizioni e *call center*	2
Garante per la protezione dei dati personali	2
Totale	**6**

Grafico delle tipologie dei riscontri resi a interessati e richiedenti



13. Tipologie di notificazioni pervenute nel 2012

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL 2012 (1)			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE
Prima notificazione al Garante	35	725	760
Modifica di una precedente notificazione	10	223	233
Notificazione della cessazione del trattamento	6	54	60
Totale	**51**	**1.002**	**1.053**

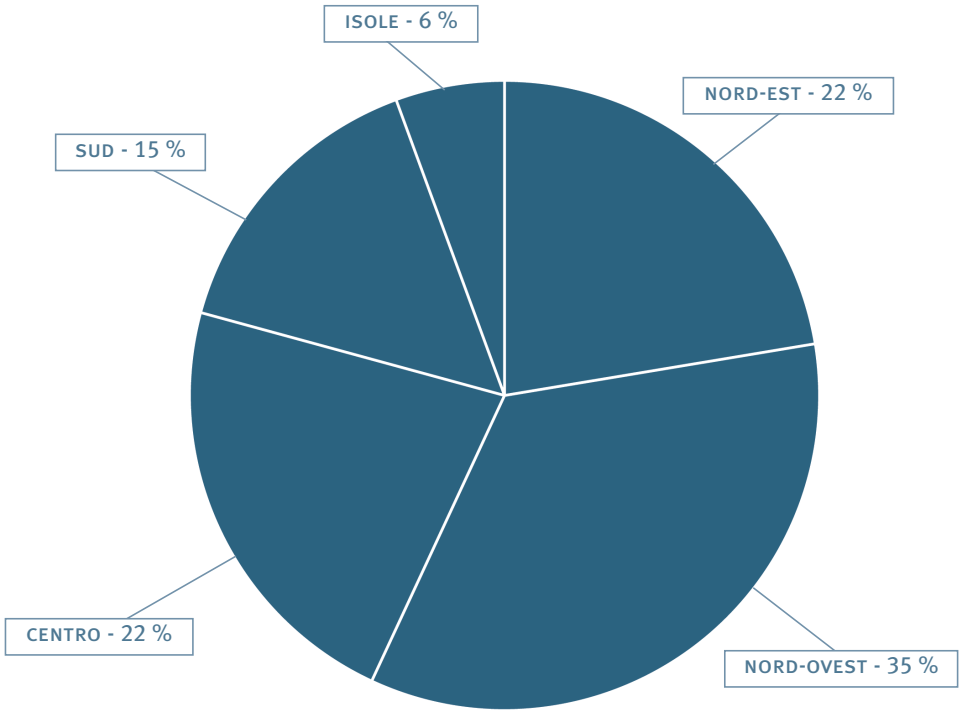
(1) I valori sono riferiti alla data del 31 dicembre 2012

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL PERIODO 2004-2012 (1)			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE
Prima notificazione al Garante	1.160	16.278	17.438
Modifica di una precedente notificazione	117	2.815	2.932
Notificazione della cessazione del trattamento	67	590	657
Totale	**1.344**	**19.683**	**21.027**

14. Tipologie di notificazioni pervenute nel periodo 2004-2012

PROVENIENZA GEOGRAFICA DELLE NOTIFICAZIONI: 2004-2012	
ITALIA	
ZONE GEOGRAFICHE	PERVENUTE
Nord-Est	4.679
Nord-Ovest	7.225
Centro	4.666
Sud	3.171
Isole	1.170
Totale	**20.911**
Da altri Paesi	116

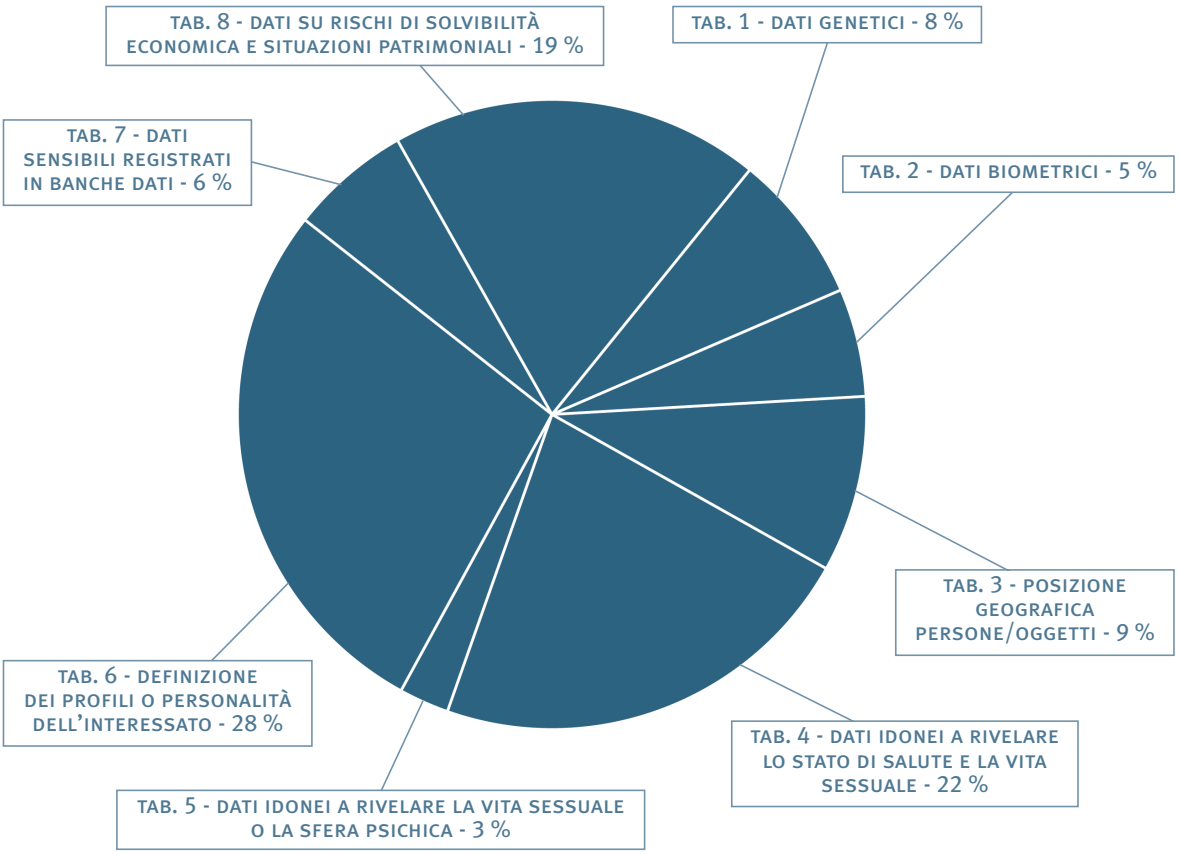
15. Provenienza geografica delle notificazioni: 2004-2012 (tabella e grafico)



(1) I valori sono riferiti alla data del 31 dicembre 2012

16. Suddivisione delle notificazioni per tipologia di trattamento svolto 2004-2012 (tabella e grafico)

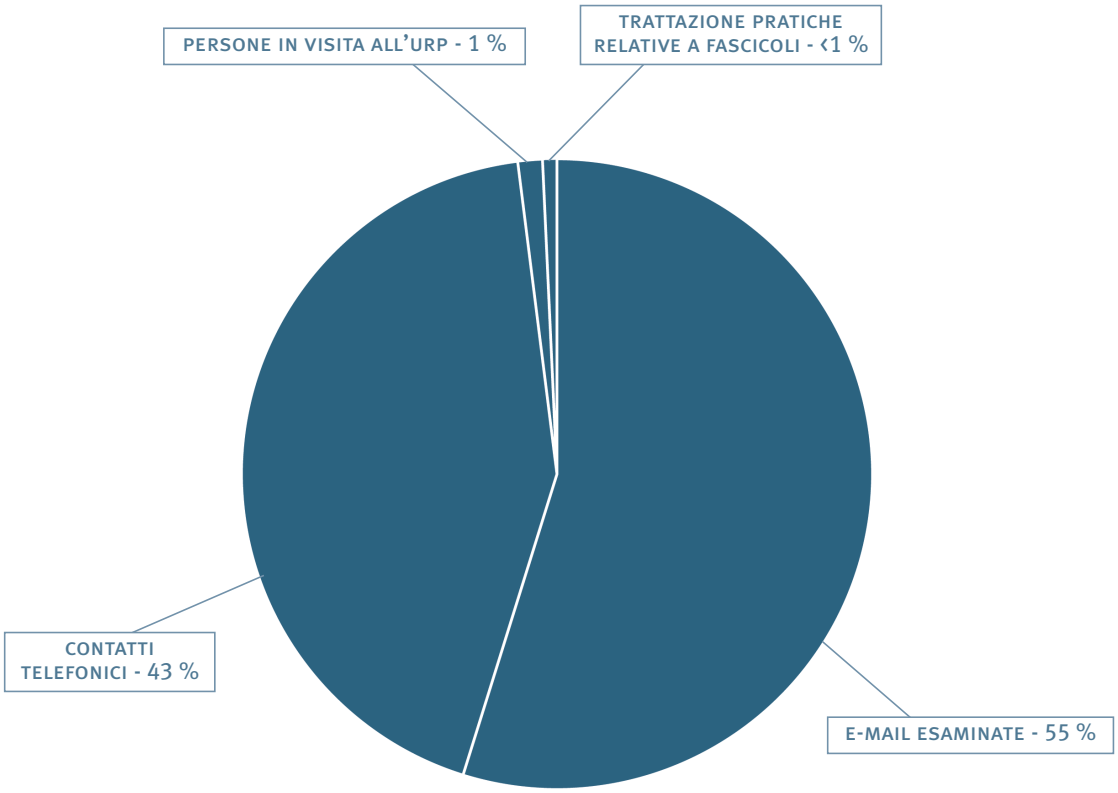
SUDDIVISIONE DELLE NOTIFICAZIONI PER TIPOLOGIA DI TRATTAMENTO SVOLTO 2004-2012	
TABELLE DI NOTIFICAZIONE COMPILATE (1)	NUMERO
Tabella 1 - Trattamento di dati genetici	2.389
Tabella 2 - Trattamento di dati biometrici	1.721
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	2.811
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	6.907
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	799
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	8.574
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	1.929
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	5.899
Totale	**31.029**



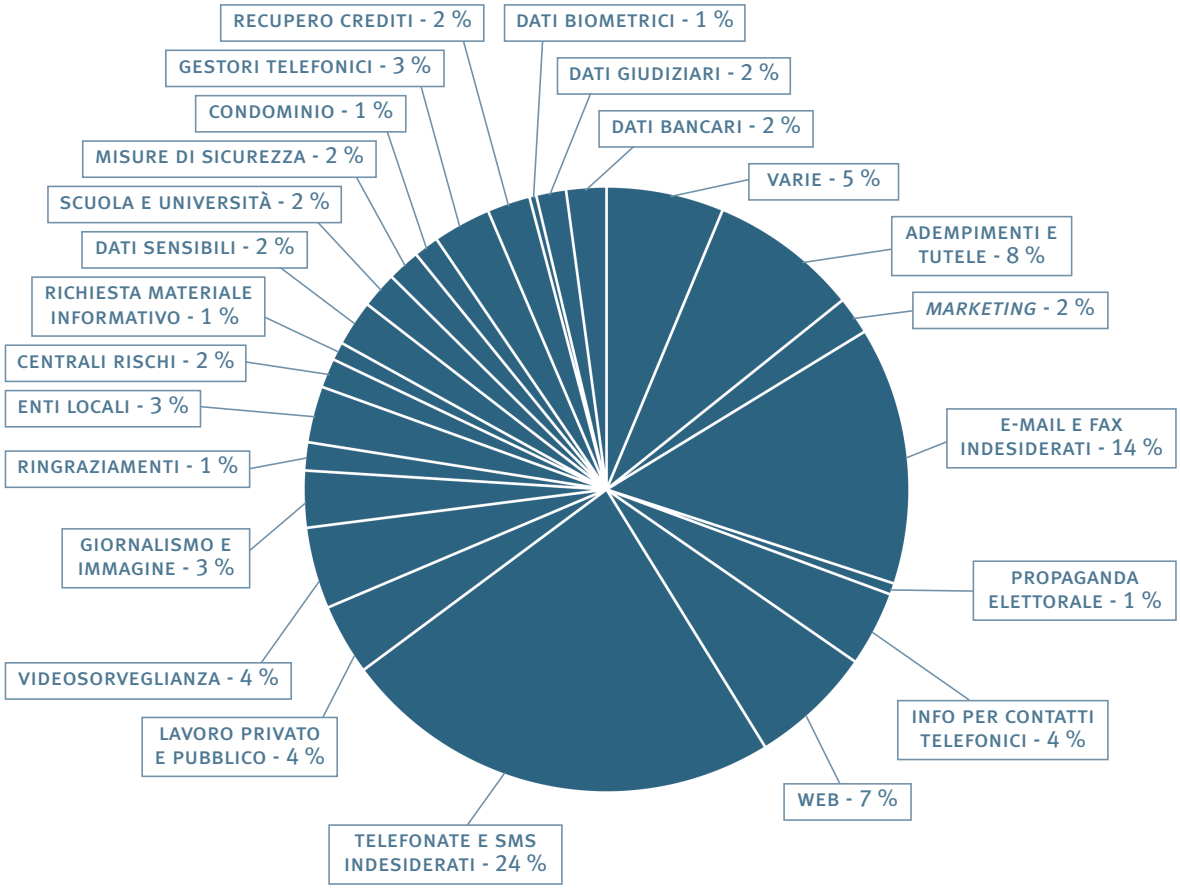
(1) Situazione alla data del 31 dicembre 2012

17. Ufficio relazioni con il pubblico (tabella e grafico)

UFFICIO RELAZIONI CON IL PUBBLICO	
	2012
E-mail esaminate	19.000
Contatti telefonici	14.969
Persone in visita all'Urp	437
Trattazione pratiche relative a fascicoli	254
Totale	**34.660**



18. E-mail esaminate dall'Ufficio relazioni con il pubblico [grafico delle categorie]



19. Posti previsti in organico

POSTI PREVISTI IN ORGANICO	
Segretario generale	1
Dirigenti	24
Funzionari	69
Operativi	30
Esecutivi	1
Totale	**125**
Personale a contratto	20

20. Personale in servizio

PERSONALE IN SERVIZIO (1)				
AREA	IN RUOLO (A)	IN POSIZIONE DI FUORI RUOLO (B)	COMANDATO PRESSO ALTRE AMMINISTRAZIONI O IN ASPETTATIVA (C)	IMPIEGATO DALL'UFFICIO (A+B-C)
Segretario generale	1			1
Dirigenti	14	4		18
Funzionari	61	3	4	60
Operativi	25			25
Esecutivi				0
Totali	**101**	7	4	**104**
Personale a contratto				18

21. Risorse finanziarie

RISORSE FINANZIARIE						
ENTRATE ACCERTATE	ANNO 2012		ANNO 2011		DIFFERENZA	
Correnti		23.571.012		23.779.047		-208.035
di cui trasferimento dallo Stato	8.856.462		8.532.693		323.769	
Totale entrate		**23.571.012**		**23.779.047**		**-208.035**
SPESE IMPEGNATE	ANNO 2012		ANNO 2011		DIFFERENZA	
Funzionamento		19.117.292		18.542.326		574.966
Capitale		338.847		420.528		-81.681
Rimborsi al Mef		251.735		251.735		–
Totale spese		**19.707.874**		**19.214.589**		**493.285**

(1) Situazione alla data del 31 dicembre 2012

Documentazione

IV. Documentazione

25. Provvedimenti del Garante

PROVVEDIMENTI DI PARTICOLARE RILIEVO

Parere del Garante su uno schema di Convenzione tra il Ministero dell'interno e l'Inps per l'accesso delle forze di polizia, tramite il Ced, alla banca dati dell'Istituto, attraverso l'utilizzo di specifiche applicazioni informatiche
2 febbraio 2012 [doc. web n. 1875293]

Parere del Garante all'Istat sullo schema di Piano generale del 9° Censimento generale dell'industria e dei servizi e del Censimento delle istituzioni *non profit*
9 febbraio 2012 [doc. web n. 1876517]

Parere del Garante al Ministro dello sviluppo economico e delle infrastrutture e dei trasporti in ordine a uno schema di decreto legislativo recante attuazione della Direttiva n. 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009
29 marzo 2012 [doc. web n. 1893400]

Trattamenti di dati per attività di propaganda elettorale - esonero dall'informativa
5 aprile 2012 [doc. web n. 1885765]

Comunicazione dei dati contabili all'Anagrafe tributaria da parte di banche e operatori finanziari: parere all'Agenzia delle entrate sulle modalità di trasmissione e di conservazione dei dati
17 aprile 2012 [doc. web n. 1886775]

Partecipazione all'accertamento fiscale e contributivo da parte dei comuni: parere del Garante sul nuovo provvedimento dell'Agenzia delle entrate
17 aprile 2012 [doc. web n. 1886825]

Immagini di persone arrestate: illecita la diffusione se raccolte all'interno della propria abitazione privata
18 maggio 2012 [doc. web n. 1900914]

Parere del Garante su uno schema di decreto interministeriale riguardante "Regole tecniche e di sicurezza relative al permesso di soggiorno conforme al Regolamento (CE) n. 1030/2002 come modificato dal Regolamento (CE) n. 380/2008"
5 giugno 2012 [doc. web n. 1908393]

Parere del Garante su uno schema di Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze riguardante l'accesso da parte delle forze di polizia, tramite il Ced del Dipartimento della pubblica sicurezza, al Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf)
12 luglio 2012 [doc. web n. 1915461]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni
19 luglio 2012 [doc. web n. 2065905]

Linee-guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali - consultazione pubblica
26 luglio 2012 [doc. web n. 1915485]

Parere del Garante su una versione aggiornata dello schema tipo di regolamento per il trattamento di dati personali sensibili e giudiziari da effettuarsi presso le regioni e le province autonome, le aziende sanitarie, gli enti e agenzie regionali/provinciali, gli enti vigilati dalle regioni e dalle province autonome
26 luglio 2012 [doc. web n. 1915390]

Lavoro: operatori di un *call center* e controlli di qualità
1° agosto 2012 [doc. web n. 1923325]

Parere del Garante su uno schema di regolamento recante norme per il funzionamento del Registro dei tumori del Veneto
13 settembre 2012 [doc. web n. 1927415]

Programma statistico nazionale 2011-2013. Aggiornamento 2013
20 settembre 2012 [doc. web n. 2069239]

Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011
20 settembre 2012 [doc. web n. 2094932]

Impiego di sistemi di videosorveglianza in un'azienda
4 ottobre 2012 [doc. web n. 2066968]

Protocollo informatico e protezione dei dati personali dei lavoratori
11 ottobre 2012 [doc. web n. 2097560]

Parere su uno schema di decreto per la consultazione del Sistema informativo Casellario (SiC) da parte di pp.aa. e gestori pubblici servizi
11 ottobre 2012 [doc. web n. 2091248]

Consegna di comunicazioni ai lavoratori e misure per prevenire la conoscibilità ingiustificata di dati personali
18 ottobre 2012 [doc. web n. 2174351]

Notifica di determinazioni aventi ad oggetto l'irrogazione di sanzioni disciplinari e misure per prevenire la conoscibilità ingiustificata di dati personali
18 ottobre 2012 [doc. web n. 2174582]

Trattamenti di dati personali effettuati mediante un sistema di videosorveglianza
25 ottobre 2012 [doc. web n. 2212623]
25 ottobre 2012 [doc. web n. 2212826]
17 gennaio 2013 [doc. web n. 2291893]

Parere del Garante su uno schema di disegno di legge sulla ratifica ed esecuzione dell'Accordo tra la Repubblica italiana e lo Stato di Israele sulla previdenza sociale
25 ottobre 2012 [doc. web n. 2185056]

Elezioni primarie 2012 e trattamento di dati personali
31 ottobre 2012 [doc. web n. 2079275]

Le attestazioni di stato civile non devono riportare annotazioni sulle adozioni
8 novembre 2012 [doc. web n. 2187244]

Trattamento eccedente dell'immagine di dipendenti pubblici
15 novembre 2012 [doc. web n. 2185342]
15 novembre 2012 [doc. web n. 2247923]

Comunicazioni all'Anagrafe tributaria da parte di banche e operatori finanziari: parere sulle modalità di trasmissione e di conservazione dei dati
15 novembre 2012 [doc. web n. 2099774]

No alle annotazioni di rettificazione di sesso su diplomi e certificazioni di laurea
15 novembre 2012 [doc. web n. 2121695]

Avvio di una consultazione pubblica ai sensi dell'art. 122 volta ad individuare modalità semplificate per l'informativa di cui all'art. 13, comma 3, del Codice in materia di protezione dei dati personali
22 novembre 2012 [doc. web n. 2139697]

Trattamento di dati sensibili riferiti ai partecipanti ad una manifestazione sindacale
29 novembre 2012 [doc. web n. 2192643]

Trattamento di dati personali connesso all'installazione di un sistema di rilevamento dati e di registrazione di immagini su veicoli del trasporto pubblico locale
29 novembre 2012 [doc. web n. 2257616]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni
20 dicembre 2012 [doc. web n. 2286432]
24 gennaio 2013 [doc. web n. 2286820]

Provvedimento prescrittivo al Ministero delle infrastrutture e dei trasporti sulle operazioni nel sistema dell'Anagrafe degli abilitati alla guida
24 gennaio 2013 [doc. web n. 2256617]

Trattamento di dati biometrici per finalità di rilevazione delle presenze dei dipendenti: verifica preliminare
31 gennaio 2013 [doc. web n. 2304669]

RAPPORTI CON IL PARLAMENTO ED ALTRE ISTITUZIONI

Parere del Garante al Ministro della salute in ordine a uno schema di decreto recante "Modifiche al decreto del Ministro del lavoro, della salute e delle politiche sociali del 17 dicembre 2008, pubblicato nella Gazzetta Ufficiale n. 9 del 13 gennaio 2009, recante 'Istituzione del sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza sanitaria in emergenza-urgenza'"
21 marzo 2012 [doc. web n. 1892560]

Parere del Garante al Ministero della salute su uno schema di decreto concernente "Modifiche al decreto del Ministro del lavoro, della salute e delle politiche sociali del 17 dicembre 2008, recante 'Istituzione del sistema informativo per il monitoraggio dell'assistenza domiciliare'"
29 marzo 2012 [doc. web n. 1893476]

Parere del Garante su uno schema di decreto del Ministro della salute concernente "Modifiche al decreto del Ministro del lavoro, della salute e delle politiche sociali recante 'Istituzione della banca dati finalizzata alla rilevazione delle prestazioni residenziali e semiresidenziali'"
17 aprile 2012 [doc. web n. 1907937]

Parere del Garante: modifiche al decreto del Ministro della salute recante "Istituzione del flusso informativo delle prestazioni farmaceutiche effettuate in distribuzione diretta o per conto, come modificato dal decreto del Ministero del lavoro, della salute e delle politiche sociali 13 novembre 2008"
11 maggio 2012 [doc. web n. 1900890]

Prove di ammissione ai corsi di laurea ad accesso programmato per l'anno accademico 2012/2013
28 giugno 2012 [doc. web n. 1912937]

Parere del Garante su uno schema di ordinanza recante disposizioni urgenti dirette a fronteggiare gli eventi sismici verificatisi il 22 e il 29 maggio nel territorio di alcune province dell'Emilia-Romagna, della Lombardia e del Veneto
2 luglio 2012 [doc. web n. 1913546]

Parere del Garante su uno schema di decreto del Presidente della Repubblica recante la disciplina del fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso, delle richieste estorsive e dell'usura
5 luglio 2012 [doc. web n. 1913538]

Parere del Garante - revisione legale dei conti annuali e dei conti consolidati mediante utilizzo delle tecnologie dell'informazione e della comunicazione
20 settembre 2012 [doc. web n. 2068734]

Trasmissione per via telematica di dati e informazioni sul ritiro dalla circolazione di banconote e monete euro sospette di falsità
4 ottobre 2012 [doc. web n. 2067279]

Parere del Garante su uno schema di decreto ministeriale riguardante la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive
18 ottobre 2012 [doc. web n. 2099252]

Parere del Garante al Mef su uno schema di regolamento per l'uso degli strumenti informatici e telematici nell'ambito del processo tributario
8 novembre 2012 [doc. web n. 2185215]

Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri recante il regolamento per la revisione delle modalità di determinazione e i campi di applicazione dell'Isee
22 novembre 2012 [doc. web n. 2174496]

Parere del Garante sullo schema di provvedimento del Direttore generale della Direzione generale per gli italiani all'estero e le politiche migratorie riguardante "Specifiche tecniche di sicurezza del processo di emissione del passaporto elettronico"
22 novembre 2012 [doc. web n. 2222980]

Parere del Garante su uno schema di decreto in materia di consegna, da parte delle aziende sanitarie del Servizio sanitario nazionale, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali
6 dicembre 2012 [doc. web n. 2223206]

Parere del Garante su uno schema di decreto recante norme in materia di sperimentazione finalizzata alla proroga del programma "carta acquisti"
6 dicembre 2012 [doc. web n. 2216848]

Trattamenti dati per attività di propaganda elettorale - esonero dall'informativa
10 gennaio 2013 [doc. web n. 2181429]

IL GARANTE E LE PUBBLICHE AMMINISTRAZIONI

Anagrafe tributaria: sicurezza e accessi - proroga degli adempimenti
16 febbraio 2011 [doc. web n. 1793806]

Sistema *Rfid* per il controllo degli ingressi e delle uscite dalle zone a traffico limitato (ztl) dei veicoli adibiti al trasporto delle merci - verifica preliminare
2 febbraio 2012 [doc. web n. 1875840]

Prescrizioni del Garante per la pubblicazione di deliberazioni contenenti dati personali sull'albo pretorio *online* di un comune
23 febbraio 2012 [doc. web n. 1876679]

Parere del Garante alla Provincia di Trento sul regolamento per il trattamento di dati sensibili e giudiziari nell'ambito del sistema educativo di istruzione e formazione provinciale
29 marzo 2012 [doc. web n. 1892028]

Installazione di un sistema di videosorveglianza per finalità di sicurezza urbana - verifica preliminare
7 aprile 2011 [doc. web n. 1811897]
18 ottobre 2012 [doc. web n. 2138277]

Parere del Garante al Ministero della salute sullo schema di accordo tra il Ministro della salute, le regioni e le Province Autonome di Trento e di Bolzano, le province, i comuni e le comunità montane sulla prevenzione degli effetti delle ondate di calore
18 maggio 2012 [doc. web n. 1900390]

Riscossione: differimento del provvedimento del 7 ottobre 2009
12 luglio 2012 [doc. web n. 1913804]

Pubblicazione sul sito web di una asl di documenti idonei a rivelare lo stato di salute
22 novembre 2012 [doc. web n. 2194472]

Diffusione sul sito web istituzionale di un comune di dati idonei a rivelare lo stato di salute
29 novembre 2012 [doc. web n. 2192671]

Diffusione sul sito web istituzionale di una scuola di dati personali relativi agli studenti
6 dicembre 2012 [doc. web n. 2217211]

Vietato riportare nella documentazione fotografica comprovante violazioni in materia di circolazione stradale immagini di soggetti non coinvolti
13 dicembre 2012 [doc. web n. 2185265]

Parere del Garante sulla deliberazione dell'Avcp attuativa dell'art. 6-*bis* del Codice dei contratti pubblici relativi a lavori, servizi e forniture (d.lgs. 12 aprile 2006, n. 163)
19 dicembre 2012 [doc. web n. 2171106]

Diffusione sul sito web di un'azienda regionale per il diritto allo studio universitario di dati relativi allo stato di disabilità
19 dicembre 2012 [doc. web n. 2223692]

Parere del Garante all'Istituto superiore di sanità in ordine alle modifiche e integrazioni apportate al regolamento per i trattamenti di dati sensibili e giudiziari emanato il 17 luglio 2007
17 gennaio 2013 [doc. web n. 2298929]

Parere al Miur sullo schema di accordo per l'integrazione delle anagrafi regionali degli studenti con l'Anagrafe nazionale degli studenti
24 gennaio 2013 [doc. web n. 2304850]

Comunicazione all'archivio dei rapporti finanziari - misure di sicurezza
31 gennaio 2013 [doc. web n. 2268436]

LA SANITÀ

Strutture sanitarie private: informativa chiara e consenso specifico per trattare i dati dei pazienti
9 febbraio 2012 [doc. web n. 1875016]

Dati sanitari: verificare l'identità dell'interessato prima di consegnare il referto medico
1° marzo 2012 [doc. web n. 1893694]

Informativa per i pazienti di uno studio radiologico: serve una chiara indicazione dei soggetti ai quali i dati possono essere comunicati e per quali finalità
15 marzo 2012 [doc. web n. 1893708]

Autorizzazione al trattamento dei dati di pazienti per una sperimentazione clinica senza consenso informato
25 ottobre 2012 [doc. web n. 2120934]

Parere del Garante su modifiche e integrazioni ad uno schema tipo di regolamento per il trattamento di dati personali sensibili e giudiziari da effettuarsi presso regioni e province autonome, aziende sanitarie, enti e agenzie regionali/provinciali, enti vigilati da regioni e province autonome
8 novembre 2012 [doc. web n. 2216879]

Trattamento dei dati personali attraverso un sistema *Rfid* di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi - verifica preliminare richiesta da un'azienda ospedaliera
29 novembre 2012 [doc. web n. 2276103]

Autorizzazione n. 2/2012 - autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale
13 dicembre 2012 [doc. web n. 2158850]

Autorizzazione n. 9/2012 - autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica
13 dicembre 2012 [doc. web n. 2159932]

I DATI GENETICI

Autorizzazione n. 8/2012 - autorizzazione generale al trattamento dei dati genetici
13 dicembre 2012 [doc. web n. 2157564]

LA STATISTICA

Istat: Censimento generale della popolazione e delle abitazioni e trattamento di dati sensibili
16 febbraio 2011 [doc. web n. 1797064]

Istat: Censimento generale della popolazione e delle abitazioni e trattamento di dati sensibili - presa d'atto del Garante
23 marzo 2011[doc. web n. 1801731]

Programma statistico nazionale 2012-2013
21 luglio 2011 [doc. web n. 1829659]

L'ATTIVITÀ DI POLIZIA

Trattamento dei dati effettuato in attuazione della Convenzione di applicazione dell'Accordo di Schengen presso le Divisioni N-Sis e Sirene del Dipartimento della pubblica sicurezza del Ministero dell'interno - differimento per l'adempimento alle prescrizioni del Garante
24 gennaio 2013 [doc. web n. 2324763]

L'ATTIVITÀ GIORNALISTICA

Archivio *online* - diritto all'oblio
12 aprile 2012 [doc. web n. 1894581]
4 ottobre 2012 [doc. web n. 2104293]

Divieto della diffusione in servizi giornalistici di immagine lesiva della dignità e della riservatezza personale
5 giugno 2012 [doc. web n. 1912974]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni
18 ottobre 2012 [doc. web n. 2130029]

Pubblicazione di sms eventualmente idonei a rivelare abitudini sessuali
13 dicembre 2012 [doc. web n. 2142715]

IL TRATTAMENTO DI DATI PERSONALI ATTRAVERSO INTERNET

Trattamento illecito di dati da parte di una società che opera nel settore del *telemarketing*
11 ottobre 2012 [doc. web n. 2089777]

Invio di comunicazioni promozionali indesiderate mediante posta elettronica
20 dicembre 2012 [doc. web n. 2223607]

IL TRATTAMENTO DI DATI NEL SETTORE DELLE COMUNICAZIONI ELETTRONICHE

Vietato l'invio di fax promozionali in assenza di una idonea informativa e di un consenso specifico
21 marzo 2012 [doc. web n. 1895176]

Trattamento di dati personali tratti da un questionario *online* in assenza di validi consenso e informativa. Ne risponde anche l'acquirente di liste di contatti da utilizzare a fini di *marketing*, indipendentemente dalla sua qualificazione giuridica nel contratto di fornitura
5 aprile 2012 [doc. web n. 1891156]

Comunicazione di dati dall'Inps al Ministero del lavoro per la ricostruzione del *curriculum* professionale di particolari categorie di lavoratori
21 marzo 2012 [doc. web n. 1885290]

Illecita la pubblicazione sul sito web di un ateneo dei dati relativi alla revoca di un contratto di insegnamento
12 aprile 2012 [doc. web n. 1896533]

Trattamento di dati personali mediante sistemi di localizzazione
1° agosto 2012 [doc. web n. 1923293]

Trattamento dei dati biometrici riferiti ai lavoratori presso un cantiere edile
13 settembre 2012 [doc. web n. 1927456]

Pubblicazione sul sito web istituzionale di un comune dei dati personali contenuti nella graduatoria provvisoria di un concorso
6 dicembre 2012 [doc. web n. 2223278]

Autorizzazione n. 1/2012 - autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro
13 dicembre 2012 [doc. web n. 2158817]

LE ATTIVITÀ ECONOMICHE

Videosorveglianza - verifica preliminare
12 gennaio 2012 [doc. web n. 1875004]
8 marzo 2012 [doc. web n. 1891026]
15 marzo 2012 [doc. web n. 1893742]
21 marzo 2012 [doc web n. 1893723]

Dati biometrici: illecito raccogliere e utilizzare le impronte digitali degli iscritti per l'accesso ad una palestra
16 febbraio 2012 [doc. web n. 1894570]
29 marzo 2012 [doc. web n. 1891999]

Esonero dall'obbligo di rendere l'informativa in forma individuale ai dipendenti ed ai clienti acquisiti attraverso la cessione di un ramo d'azienda
5 luglio 2012 [doc. web n. 1913790]

Installazione di un sistema completamente automatizzato di cassette di sicurezza - verifica preliminare
13 settembre 2012 [doc. web n. 1927441]

Sistema di rilevazione di dati biometrici dei passeggeri - verifica preliminare
4 ottobre 2012 [doc. web n. 2059743]

Sistema per l'accesso della clientela - verifica preliminare
18 ottobre 2012 [doc. web n. 2212554]

Istanza di bilanciamento di interessi
24 gennaio 2013 [doc. web n. 2352902]

Sistemi di rilevazione biometrica - verifica preliminare
31 gennaio 2013 [doc. web n. 2311886]
31 gennaio 2013 [doc. web n. 2304808]

IL TRASFERIMENTO DEI DATI ALL'ESTERO

Autorizzazione - trasferimento verso gli USA di dati personali relativi ai dipendenti
11 ottobre 2012 [doc. web n. 2111613]

Clausole contrattuali tipo e trasferimento dei dati all'estero tramite responsabile stabilito in UE
15 novembre 2012 [doc. web n. 2191156]

LE LIBERE PROFESSIONI

Provvedimento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali
21 aprile 2011 [doc. web n. 1809039]

Autorizzazione al trattamento dei dati sensibili nell'attività di mediazione finalizzata alla conciliazione delle controversie civili e commerciali
21 aprile 2011 [doc. web n. 1808658]

Autorizzazione al trattamento dei dati a carattere giudiziario correlato all'attività di mediazione finalizzata alla conciliazione delle controversie civili e commerciali
21 aprile 2011[doc. web n. 1808676]

Ordini professionali: diffusione via internet di dati giudiziari riferiti a iscritti
17 gennaio 2013 [doc. web n. 2315622]

LA TRATTAZIONE DEI RICORSI

Accesso dell'interessato ai propri dati
8 marzo 2012 [doc. web n. 1889056]
20 settembre 2012 [doc. web n. 2106524]

Archivio *online* - diritto all'oblio
8 marzo 2012 [doc. web n. 1887094]

Ambito di applicazione del Codice
15 marzo 2012 [doc. web n. 1889091]

Diritto di accesso ai dati di persona deceduta
21 marzo 2012 [doc. web n. 1889154]
26 luglio 2012 [doc. web n. 2104639]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni
4 ottobre 2012 [doc. web n. 2108032]

Accesso dell'interessato e contenzioso giurisdizionale
11 ottobre 2012 [doc. web n. 2131862]

Ricorso al Garante - legittimazione passiva
15 novembre 2012 [doc. web n. 2286264]

Ricorso al Garante - urgenza
29 novembre 2012 [doc. web n. 2248935]

Accesso dell'interessato e diritto di difesa
29 novembre 2012 [doc. web n. 2286291]

Ambito di applicazione del Codice - persone giuridiche
19 dicembre 2012 [doc. web n. 2286411]

L'ATTIVITÀ ISPETTIVA E LE SANZIONI

Ordinanza di ingiunzione nei confronti di una società
15 marzo 2012 [doc. web n. 2115627]
15 ottobre 2012 [doc. web n. 2368171]

26. Principali attività internazionali

UNIONE EUROPEA

REVISIONE DELLA DIRETTIVA N. 95/46/CE

Comunicazione(2012) 11 della Commissione - Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)
25 gennaio 2012 [doc. web n. 1895611]

Comunicazione(2012) 10 della Commissione - Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati
25 gennaio 2012 [doc. web n. 1895615]

GRUPPO ART. 29

WP 190 - Programma di lavoro 2012-2013
1° febbraio 2012 [doc. web n. 2375271]

WP 191 - Parere 01/2012 sulle proposte di riforma in materia di protezione dei dati
23 marzo 2012 [doc. web n. 2375522]

WP 192 - Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi *online* e mobili
22 marzo 2012 [doc. web n. 2375284]

WP 193 - Parere 03/2012 sugli sviluppi nelle tecnologie biometriche
27 aprile 2012 [doc. web n. 2375294]

WP 194 - Parere 04/2012 relativo all'esenzione dal consenso per l'uso di *cookie*
7 giugno 2012 [doc. web n. 2133013]

WP 195 - Documento di lavoro 02/2012 sulle *Bcr for processor* (responsabili del trattamento)
6 giugno 2012 [doc. web n. 2375532]

WP 196 - Parere 05/2012 sul *cloud computing*
1° luglio 2012 [doc. web n. 2133003]

WP 198 - Parere 07/2012 sul livello di protezione dei dati personali nel Principato di Monaco
19 luglio 2012 [doc. web n. 2133808]

WP 199 - Parere 08/2012 che fornisce un ulteriore contributo alle discussioni sulla riforma in materia di protezione dei dati
5 ottobre 2012 [doc. web n. 2133818]

Lettera del Gruppo Art. 29 alla Vicepresidente Reding relativa alle implicazioni sul *budget* e sulle risorse delle autorità di protezione dati alla luce delle proposte di riforma della Commissione in materia di protezione dei dati
4 aprile 2012 [doc. web n. 2375399]

Lettera del Gruppo Art. 29 alla Commissaria Malmström su "*smart borders*" (frontiere intelligenti)
12 giugno 2012 [doc. web n. 2377470]

Lettera del Gruppo Art. 29 alla Commissaria Malmström sulla proposta di regolamento che istituisce il Sistema europeo di sorveglianza delle frontiere (Eurosur)
12 giugno 2012 [doc. web n. 2375181]

Lettera del Gruppo Art. 29 a Mr. Zourek, Direttore generale della DG Fiscalità e Unione doganale della Commissione in merito al *Foreign Account Tax Compliance Act* (FATCA)
21 giugno 2012 [doc. web n. 2375072]

Lettera del Gruppo Art.29 a Google Inc. riguardante le modifiche apportate alla propria *privacy policy*
Allegate raccomandazioni del Gruppo Art. 29 a Google Inc.
16 ottobre 2012 [doc. web nn. 2375141 e 2375151]

Lettera del Gruppo Art. 29 indirizzata a Ms. Le Bail, Direttore generale della DG Giustizia della Commissione riguardante l'Autorità di vigilanza degli Stati Uniti sulle revisioni contabili (PCAOB)
13 dicembre 2012 [doc. web n. 2375161]

34ma CONFERENZA DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Dichiarazione sul *profiling*
26 ottobre 2012 [doc. web n. 2375042]

Risoluzione sul *cloud computing*
26 ottobre 2012 [doc. web n. 2375241]

Risoluzione sul futuro della *privacy*
26 ottobre 2012 [doc. web n. 2375251]

SPRING CONFERENCE

Risoluzione sul pacchetto di riforma di protezione dati
3-4 maggio 2012 [doc. web n. 2375261]

AUTORITÀ COMUNE DI CONTROLLO EUROPOL

Dichiarazione pubblica sulla seconda ispezione riguardante l'accordo Tftp
Comunicato stampa
21 marzo 2012 [doc. web nn. 2375320 e 2375032]

Parere riguardante la proposta di modifica del regolamento Eurodac
10 ottobre 2012 [doc. web n. 2375211]

Parere 12-09 sul livello di protezione dati in Liechtenstein
6 febbraio 2012 [doc. web n. 2381001]

Parere 12-83 sul livello di protezione dati in Serbia
10 dicembre 2012 [doc. web n. 2375221]

AUTORITÀ COMUNE DI CONTROLLO SCHENGEN

Lettera alla Commissaria Malmström su divieti di ingresso e segnalazioni *ex* art. 96
11 dicembre 2012 [doc. web n. 2375381]

GRUPPO DI COORDINAMENTO E SUPERVISIONE EURODAC

Rapporto di attività 2010-2011
24 maggio 2012 [doc. web n. 2375052]

GRUPPO DI LAVORO INTERNAZIONALE SULLA PROTEZIONE DEI DATI NEL SETTORE DELLE TELECOMUNICAZIONI - IWGDPT

Documento di lavoro cd. "*sopot memorandum*" sul *cloud computing*
24 aprile 2012 [doc. web n. 2375062]

CONSIGLIO D'EUROPA

Documento sulla modernizzazione della Convenzione n. 108/1981
29 novembre 2012 [doc. web n. 2375191]

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it
e-mail: garante@garanteprivacy.it

progetto grafico:
Emiliano Germani

stampa:
Istituto Arti Grafiche Mengarelli s.n.c.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI