SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Doc.**CXXXVI**
n. **4**

RELAZIONE
SULL'ATTIVITÀ SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(ANNO 2010)

(Articolo 154, comma 1, lettera m), del codice di cui al decreto legislativo 30 giugno 2003, n. 196)

Presentata dal garante per la protezione dei dati personali

(PIZZETTI)

Comunicata alla Presidenza il 6 settembre 2011

PAGINA BIANCA

INDICE

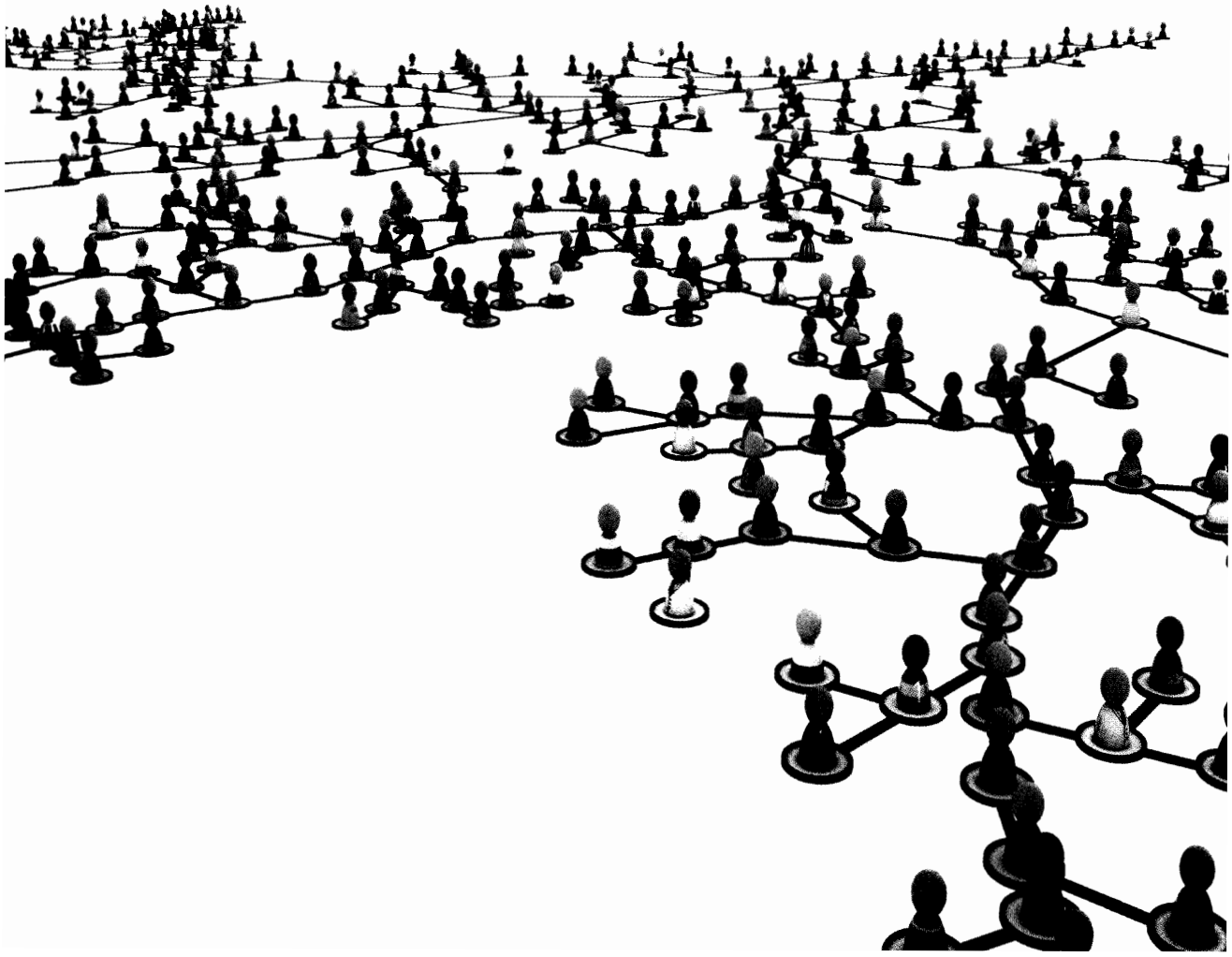
INDICE

ELENCO DELLE ABBREVIAZIONI

La presente Relazione è riferita al 2010 e contiene talune notizie già anticipate nella precedente edizione, nonché alcune ulteriori informazioni, aggiornate al 2 marzo 2011, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	*ad esempio*
art.	*articolo*
c.c.	*codice civile*
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



PAGINA BIANCA

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

1. Principali interventi dell'Autorità nel 2010

1.1. Provvedimenti più significativi

1.1.1. Trattamenti collegati allo svolgimento di funzioni di giustizia

Nel periodo di riferimento l'applicazione della normativa sulla protezione dei dati personali all'esercizio di funzioni giurisdizionali è stata oggetto di decisioni di particolare delicatezza, in relazione alle implicazioni di carattere generale, riguardanti la tutela di diritti fondamentali della persona nel quadro costituzionale dei rapporti tra poteri.

In risposta ad alcune istanze che avevano lamentato l'illecito utilizzo in giudizio di dati sensibili e giudiziari, l'Autorità ha sottolineato che, ai sensi dell'art. 160 del Codice, spetta al giudice adito pronunciarsi, in base alle pertinenti disposizioni processuali, sulla validità, l'efficacia e l'utilizzabilità di atti presentati nell'ambito del procedimento giudiziario, anche se basati su un trattamento illecito di dati personali (*Provv.* 23 settembre 2010 [doc. *web* n. 1756065]; *Provv.* 4 novembre 2010 [doc. *web* n. 1770943]; *Provv.* 17 novembre 2010 [doc. *web* n. 1779765]).

Al termine di verifiche svolte in collaborazione con il Consiglio di Stato ed il TAR del Lazio, è emerso –pur in un quadro di complessivo rispetto delle regole– che gli uffici giudiziari amministrativi dovranno accrescere le misure di sicurezza a protezione dei dati giudiziari (*Provv.* 23 settembre 2010 [doc. *web* n. 1753845]). In particolare, il Garante ha fornito specifiche indicazioni sia per il trattamento dei dati svolto senza l'ausilio di strumenti elettronici –soprattutto per una maggiore protezione dei fascicoli processuali– sia per il trattamento con l'ausilio di strumenti elettronici, specie per le modalità di accesso dei magistrati e del personale amministrativo al Nuovo sistema informativo della giustizia amministrativa (NSIGA).

L'Autorità si è altresì occupata della diffusione dei provvedimenti giurisdizionali su supporti cartacei ed informatici nonché mediante reti di comunicazione elettronica, fonte preziosa per lo studio e l'accrescimento della cultura giuridica e strumento indispensabile di controllo da parte dei cittadini dell'esercizio del potere giurisdizionale. In taluni casi, tuttavia, riportare le generalità delle parti può risultare in contrasto con esigenze di tutela della loro dignità e riservatezza.

Al riguardo, sulla base di segnalazioni e quesiti ricevuti, dopo ampia consultazione con gli operatori del settore, sono state adottate specifiche linee-guida (*Provv.* 2 dicembre 2010 [doc. *web* n. 1774813], in *G.U.* 4 gennaio 2011, n. 2) –che non si applicano all'attività giornalistica, oggetto di altra disciplina– sulla pubblicazione di atti giurisdizionali per la finalità di informazione giuridica. In sostanza sono stati individuati i casi in cui chi intende pubblicare l'atto giudiziario deve oscurare i dati delle parti e gli elementi utili ad indentificarle (in particolare ove si tratti di minori e di procedimenti relativi a rapporti di famiglia), nonché i criteri per richiedere l'"anonimizzazione"; questa, che può essere anche decisa d'ufficio dal giudice, va annotata sull'atto, in modo che chi lo riceve provveda prima di diffonderne il contenuto.

1.1.2. Pubblicazione di atti sul web *da parte di amministrazioni pubbliche*

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" (*Provv.* 2 marzo 2011 [doc. *web* n. 1793203], in *G.U.* 19 marzo 2011, n. 64), adottate dopo ampia consultazione, definiscono un quadro unitario delle misure che la p.a. deve adottare per la pubblicazione di atti e documenti sui propri siti *web* istituzionali.

In termini generali, le amministrazioni pubbliche possono mettere in rete atti o documenti contenenti dati personali solo sulla base di una previsione normativa, rispettando i princìpi di necessità, proporzionalità e pertinenza ed il generale divieto di diffondere dati sulla salute. Contro i rischi di cancellazioni e modifiche delle informazioni presenti *online* vanno adottate adeguate misure tecnologiche. La reperibilità dei documenti deve essere, se possibile, assicurata attraverso motori di ricerca interni al sito della singola amministra-

zione, allo scopo di garantire un accesso coerente con la finalità per la quale i dati sono stati resi pubblici, evitando il rischio di estrazione arbitraria dei dati, che ne renderebbe incontrollabile l'uso. Con riguardo alla conservazione *online* dei dati, in mancanza di specifiche disposizioni le pp.aa. devono individuare limiti temporali congrui alle finalità del trattamento, e provvedere successivamente a rimuoverli.

Ancora, contro i rischi di riproduzione e riutilizzo dei *file* contenenti dati personali, devono essere installati *software* e sistemi di *alert* che consentano di riconoscere e segnalare accessi anomali, al fine di mettere in atto contromisure adeguate.

1.1.3. Trattamenti di dati sensibili, in particolare relativi allo stato di salute

L'esame delle finalità per le quali è ammesso il trattamento e l'individuazione delle cautele da osservare sono stati i profili specifici oggetto di diversi provvedimenti adottati dall'Autorità in questa materia.

In un *parere* (17 novembre 2010 [doc. *web* n. 1769451]) reso alla Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei ministri, aderendo a quanto prospettato dalla Commissione stessa, il Garante ha affermato che un genitore non può accedere presso la Asl alla documentazione sanitaria della figlia minorenne che, all'insaputa del padre, si sia rivolta ad un consultorio per farsi prescrivere farmaci contraccettivi. Va infatti riconosciuta alla minore una sfera di riservatezza che garantisca effettivamente la sua autodeterminazione, e permetta l'utilizzo delle strutture autorizzate, che possono assicurare le necessarie garanzie nell'erogazione delle prestazioni.

In relazione al servizio di consegna a domicilio, offerto da un supermercato agli acquirenti invalidi o disabili, il Garante ha deciso (*Provv.* 13 maggio 2010 [doc. *web* n. 1729156]) che non può essere chiesta, a tal fine, copia del verbale di invalidità, essendo sufficiente che la persona, al momento della prima richiesta del servizio, esibisca un qualsiasi documento che attesti il suo stato. Il trattamento dei dati è quindi risultato sproporzionato rispetto alle finalità perseguite ed al punto vendita oggetto della segnalazione l'Autorità ha anche prescritto di distruggere le copie dei verbali medici già acquisite.

Oggetto di un altro *provvedimento* (19 gennaio 2011 [doc. *web* n. 1787877]) sono state

le modalità con cui fornire agli interessati l'informativa in relazione ad un progetto di sorveglianza epidemiologica dei tumori nella popolazione militare impegnata in Bosnia-Herzegovina e nel Kosovo. Il progetto prevede in particolare che il Ministero della difesa fornisca all'Istituto superiore di sanità i dati personali dei militari (da incrociare con quelli di altre banche dati), per valutare se la permanenza nei Balcani, ove è stato fatto uso di munizioni ad uranio impoverito, abbia avuto conseguenze sulla salute dei soldati.

Per l'ingente numero delle persone coinvolte è stata prevista, in luogo dell'informativa resa a ciascun interessato, la pubblicazione della medesima sui siti del Ministero della difesa, delle singole forze armate e delle associazioni del personale in quiescenza, oltre che su due quotidiani di larga diffusione nazionale. L'Autorità, per assicurarne la massima conoscibilità, ha prescritto la pubblicazione dell'informativa anche sul sito dell'Istituto superiore di sanità e la sua agevole visibilità sino alla conclusione del progetto (art. 154, comma 1, lett. *c*), del Codice e art. 6, comma 4, del codice di deontologia e buona condotta per i trattamenti di dati per scopi statistici e scientifici).

In relazione ad una ricerca sociologica svolta tra aderenti ad un istituto religioso, con un questionario relativo, tra l'altro, ad opinioni politiche, abitudini sessuali, condizioni di salute, sono state prescritte (art. 154, comma 1, lett. *c*) e *d*), del Codice) le misure idonee ad escludere il rischio di interconnessione tra i dati in parola, raccolti da una società esterna, ed i nominativi degli aderenti all'istituto che avevano preso parte all'iniziativa; in particolare, è stata vietata la trasmissione dei questionari agli altri soggetti coinvolti nella ricerca ed ordinata la distruzione dei medesimi al termine della ricerca stessa. Ciò per impedire l'identificazione, sia pur indiretta, degli interessati, in considerazione anche del loro ristretto numero (*Provv.* 1° aprile 2010 [doc. *web* n. 1721183]).

1.1.4. Giornalismo ed informazione online

Il delicato equilibrio tra libertà di informazione e riservatezza degli interessati è stato in diverse decisioni individuato applicando il principio dell'essenzialità dell'informazione (cfr. art. 137, comma 3, del Codice e art. 6 del codice di deontologia sul trattamento dei dati nell'attività giornalistica - Allegato A.1. al Codice).

Riconoscendo che rientra nel diritto alla manifestazione del pensiero la pubblicazione di atti giudiziari non più coperti da segreto, è stata prescritta la cancellazione dei dati non essenziali riportati in un'ordinanza di custodia cautelare –numeri di telefono, recapiti e codici fiscali di diverse persone ivi citate– ad un'associazione che, a corredo di una notizia, aveva diffuso *online* il testo del *provvedimento* giudiziario (v. art. 139, comma 5, del Codice; *Provv.* 29 settembre 2010 [doc. *web* n. 1763096]).

In un altro caso è stata ritenuta di rilevante interesse pubblico la notizia, fornita dalla seguace di un'associazione in un'intervista pubblicata su un sito Internet, delle vessazioni da lei stessa subite e delle cause dei decessi di altri seguaci, talvolta con menzione delle relative patologie. L'Autorità ha però prescritto di citare le persone interessate –la cui riservatezza è meritevole di tutela anche dopo la morte– solo con nomi di fantasia, ovvero con le iniziali puntate, avendo ravvisato nella pubblicazione del loro cognome una violazione della sfera di riservatezza, del decoro e della dignità delle persone (cfr. art. 139, comma 5, del Codice; *Provv.* 1° luglio 2010 [doc. *web* n. 1738303]).

L'ulteriore diffusione, anche sul *web*, dei dati personali relativi ad alcune adozioni è stata vietata ad un'emittente televisiva (*Provv.* 6 maggio 2010 [doc. *web* n. 1718239]) in relazione ad alcune trasmissioni, nel corso delle quali erano stati forniti elementi che rendevano identificabili gli adottati, favorendone la ricerca da parte di genitori e fratelli naturali. L'Autorità ha ravvisato in tale condotta un contrasto con la *ratio* della disciplina in materia di adozioni, la quale individua specificamente i presupposti perché l'adottato possa accedere ad informazioni che riguardano la sua origine (v. artt. 27, 28, e 73, l. 4 maggio 1983, n. 184, modificata dalla l. 28 marzo 2001, n. 149) e, di conseguenza, con il Codice (v. artt. 2, 11, 137). Nei confronti dell'emittente è stato anche avviato un procedimento per applicare sanzioni pecuniarie, nonché la segnalazione all'autorità giudiziaria, poiché il blocco disposto in relazione ad una delle puntate non è stato osservato.

Nei confronti di un'altra emittente è stata vietata l'ulteriore diffusione della parte di una intervista in cui una donna, narrando gli abusi subiti in famiglia quando era minorenne, aveva fatto riferimento agli abusi subiti anche dalla sorella, minorenne al momento dell'intervista, con dati che ne consentivano l'identificazione (*Provv.* 16 settembre 2010

[doc. *web* n. 1753383]). Come più volte ribadito dal Garante (v. *Relazione* 2009, p. 7 ss.), l'obbligo del giornalista di tutelare la riservatezza dei minori, in particolare se vittime di abusi sessuali, prevale infatti sul diritto di cronaca. Ciò anche in relazione ad interviste a soggetti che liberamente rendano noti i dati relativi ai minori interessati (cfr. art. 114, comma 6, c.p.p.; art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso).

1.1.5. Comunicazioni elettroniche e acquisizioni su larga scala di immagini per la pubblicazione online

In relazione all'utilizzo massiccio di tecnologie applicate a dimensioni diverse della vita quotidiana, l'Autorità ha assunto decisioni per diversi profili innovative.

Il Garante ha bloccato (*Provv.* 9 settembre 2010 [doc. *web* n. 1750529]) qualsiasi trattamento effettuato da *Google* sui frammenti di comunicazioni elettroniche captati sul territorio italiano, tramite appositi *software*, dalle *Google car* che, per il servizio *Street View*, acquisiscono immagini panoramiche a livello stradale. Diversamente da quanto prospettato dalla Società, l'Autorità ha ritenuto che il carattere sistematico della raccolta, protrattasi per circa due anni, rende concreta l'eventualità che le informazioni, pur frammentarie, abbiano natura di dati personali. Inoltre, gli atti sono stati trasmessi all'autorità giudiziaria per l'accertamento di eventuali violazioni delle norme penali che proteggono le comunicazioni effettuate con un sistema telematico (cfr. artt. 617-*quater* e *quinquies* c.p.).

Inoltre, sempre con riferimento al servizio *Street View*, a pena di rilevanti sanzioni pecuniarie è stato prescritto (*Provv.* 15 ottobre 2010 [doc. *web* n. 1759972]) alla società californiana di fornire dettagliate informazioni sul passaggio delle *Google car*, sia sul proprio sito, sia sulle pagine di cronaca di almeno due quotidiani, sia su emittenti locali, anche per consentire agli interessati di allontanarsi dai luoghi in cui vengono riprese le immagini.

Al riguardo sono state applicate le norme del nostro ordinamento, con significativa innovazione rispetto ad alcuni casi precedenti, poiché il citato trattamento è per sua natura effettuato con strumenti situati sul territorio italiano (art. 5 del Codice), ed è stato

prescritto alla Società di nominare un proprio rappresentante in Italia, al quale i cittadini potranno rivolgersi per tutelare i loro diritti.

1.1.6. Protezione dei dati dei lavoratori dipendenti

L'utilizzo in azienda di strumenti resi disponibili dal progresso tecnologico rende di particolare rilievo l'applicazione delle disposizioni per la protezione dei dati personali. È quanto emerge dal *provvedimento* 7 ottobre 2010 [doc. *web* n. 1763071], con il quale il Garante ha bloccato la raccolta di dati effettuata da una società tramite l'installazione di sistemi di geolocalizzazione su alcune vetture aziendali. Dall'istruttoria è emerso il mancato rispetto delle disposizioni che subordinano l'installazione di apparecchiature idonee al controllo a distanza dei dipendenti al previo accordo dei sindacati o all'autorizzazione della Direzione provinciale del lavoro (art. 4, l. n. 300 del 1970). Il *provvedimento* stabilisce inoltre l'obbligo di notificare al Garante il trattamento (art. 37 ss. del Codice), ove autorizzato dalla predetta Direzione provinciale, e di nominare specifici incaricati per l'accesso ai dati acquisiti dal sistema.

1.1.7. Iniziativa economica: telemarketing *e profilazione, agenzie di* rating

I provvedimenti di carattere generale relativi al *telemarketing* adottati nel periodo di riferimento sono volti all'applicazione della nuova disciplina relativa al Registro delle opposizioni, per l'iscrizione delle utenze telefoniche degli abbonati che non desiderano ricevere telefonate promozionali.

Come ampiamente ricordato nella *Relazione* 2009 (p. 10), l'art. 20-*bis* del d.l. 25 settembre 2009, n. 135, convertito, con modificazioni, dalla l. n. 166/2009 ha ribaltato il principio della necessità del consenso esplicito per il trattamento di dati personali provenienti da elenchi pubblici effettuato mediante telefono per finalità commerciali (cd. "*opt in*"), sostituendovi la regola del necessario esercizio del diritto di opposizione da parte dell'interessato (cd. "*opt out*") da esercitarsi mediante iscrizione nell'apposito Registro.

Durante i lavori parlamentari il Garante, con un *comunicato stampa*, sottolineando i possibili effetti negativi della riforma per lo stesso *marketing* telefonico, aveva fatto presente

che registri come quello previsto dal legislatore italiano non hanno in realtà funzionato in nessuno dei Paesi in cui sono stati istituiti.

In questo quadro, l'Autorità ha comunque assicurato al Governo la collaborazione richiesta, anche sullo schema di regolamento di attuazione del nuovo sistema, recentemente adottato (d.P.R. 7 settembre 2010, n. 178; *Parere* 13 maggio 2010 [doc. *web* n. 1734800]; v. anche par. 1.2.3.).

In tale *parere* l'Autorità nel dar conto, preliminarmente, del recepimento di gran parte delle osservazioni da essa formulate in via collaborativa, ha comunque proposto di elevare ulteriormente le garanzie del diritto alla protezione dei dati personali rispetto al trattamento effettuato per finalità di *marketing*, in relazione al quadro normativo vigente, anche europeo. Ciò segnatamente per quanto riguarda le modalità di consultazione del Registro da parte degli operatori e la disciplina dell'assegnazione a ciascun operatore, da parte del gestore del Registro, delle credenziali di autenticazione e dei profili di autorizzazione, nonché la conservazione dei dati relativi a ogni operazione di accesso al sistema.

In concomitanza con l'entrata in funzione del Registro pubblico delle opposizioni –al quale il gestore (Fondazione Bordoni) deve consentire l'accesso al Garante, per l'esercizio delle funzioni di vigilanza e controllo attribuitegli dalla legge– l'Autorità ha adottato un *provvedimento* prescrittivo di carattere generale (*Provv.* 19 gennaio 2011 [doc. *web* n. 1784528], in *G.U.* 31 gennaio 2011, n. 24), in cui per assicurare il rispetto della volontà dei cittadini, ha precisato gli obblighi in capo alle imprese.

In particolare è stato chiarito che con l'entrata in funzione del Registro i numeri contenuti in banche dati comunque formate sono utilizzabili solo previo consenso *ad hoc*; la volontà espressa da un abbonato di non ricevere telefonate da una determinata impresa dev'esser rispettata, anche se l'interessato non è iscritto al Registro; il consenso alla ricezione, che il titolare del trattamento dev'esser in grado di documentare per iscritto, è sempre revocabile.

Con successivo *provvedimento* 24 febbraio 2011 [doc. *web* n. 1794638] è stato prescritto agli operatori di informare gli utenti della possibilità di iscriversi al Registro, ed è stato precisato il contenuto dei due modelli da utilizzare, l'uno per i nuovi abbonati e gli

utenti che cambiano numero, l'altro per i vecchi abbonati, indicando anche un termine per fornire al Garante assicurazione dell'avvenuto adempimento. Ciò per rendere effettivo, tramite l'informazione, il diritto di scelta degli interessati.

Il mancato rispetto di queste e delle altre prescrizioni recate dai provvedimenti comporta l'applicazione di sanzioni che, nei casi più gravi, possono raggiungere i 300.000 euro.

Sempre in materia di *marketing*, con *provvedimento* 8 aprile 2010 [doc. *web* n. 1721205] relativo all'invio, ad opera di un'agenzia di viaggi, di comunicazioni promozionali agli interessati che si erano registrati sul sito, è stato ribadito che il consenso dell'interessato è necessario per l'invio di e-mail promozionali, e che per la profilazione dei dati di navigazione è richiesto un consenso specifico, distinto rispetto a quello necessario per i trattamenti con finalità di *marketing*.

Di natura diversa il provvedimento con il quale la filiale italiana di un'agenzia di *rating* è stata autorizzata a trattare, senza il consenso degli interessati, i dati dei dipendenti e, alla luce della normativa comunitaria in materia, del loro "*nucleo familiare ristretto*", per verificare eventuali conflitti di interesse nell'attività posta in essere (*Provv.* 19 maggio 2010 [doc. *web* n. 1736161]; cfr. art. 24, comma 1, lett. *g*), del Codice). La vigente normativa statunitense richiede alla capogruppo, attiva in tutto il mondo, di certificare che l'attività, anche delle società collegate, non è influenzata da conflitti di interesse. Il Garante ha tra l'altro prescritto di fornire agli interessati un'adeguata informativa, evidenziando che qualunque dato trattato in violazione della normativa sulla *privacy* non sarà utilizzabile.

1.1.8. Trattamento di dati per la "tessera del tifoso"

Con riferimento alle misure volte a prevenire e reprimere i fenomeni di violenza connessi ad alcune competizioni sportive, il Garante ha esaminato i presupposti del trattamento dei dati previsto dal programma "tessera del tifoso", ed individuato alcune misure per renderlo conforme alle norme vigenti (*Provv.* 10 novembre 2010 [doc. *web* n. 1779725]).

In particolare, diversamente da quanto prospettato in alcune delle istanze ricevute, l'Autorità ha ritenuto che il previsto utilizzo dei dati anche giudiziari non difetti di base giuridica, alla luce delle valutazioni del Ministero dell'interno, secondo cui la tessera

costituirebbe una "facilitazione" ai sensi delle norme in materia (art. 8, d.l. 8 febbraio 2007, n. 8, convertito, con modificazioni, dalla l. 4 aprile 2007, n. 41); ha inoltre precisato che per l'adesione al programma non è richiesto il consenso, considerando il trattamento necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato (art. 24, comma 1, lett. *b*), del Codice).

In questo quadro il Garante ha però stabilito che l'informativa da fornire ai tifosi deve chiaramente distinguere i trattamenti di dati che non richiedono il consenso, da quelli che possono essere effettuati solo su base volontaria e con un consenso *ad hoc* (*marketing*, profilazione). Dovrà essere inoltre ben specificato, tra l'altro, che i dati anagrafici dei possessori delle tessere vengono comunicati alle questure allo scopo di verificare l'assenza di provvedimenti che ostacolino il rilascio delle stesse.

1.2. RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI

1.2.1. Le audizioni del Garante in Parlamento

Nel 2010 il Garante ha partecipato ad alcune audizioni presso commissioni parlamentari, permanenti e speciali, o altri organismi anche bicamerali, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge aventi riflessi in materia di protezione dei dati personali.

In questo quadro si collocano, in particolare:

a) il 9 novembre 2010, presso il Comitato parlamentare di controllo sull'attuazione dell'accordo di Schengen, di vigilanza sull'attività di EUROPOL, di controllo e vigilanza in materia di immigrazione, un'audizione nell'ambito dell'indagine conoscitiva sulle nuove politiche europee in materia di immigrazione. Nell'intervento è stato illustrato il ruolo del Garante anche come Autorità di protezione dei dati e di controllo in ambito europeo (Schengen, EUROPOL, VIS, EURODAC) e sono state evidenziate alcune criticità in sede di applicazione delle norme europee e nazionali in tali settori, ravvisando, in particolare, l'esigenza di un maggiore coordinamento delle attività svolte in tali ambiti, nonché di una maggiore funzionalità dei rapporti fra le autorità nazionali e i parlamenti;

b) il 22 settembre 2010, 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 occasione il Garante ha analizzato le possibili implicazioni, sotto il profilo della protezione dei dati personali, derivanti dall'applicazione della legge-delega 5 maggio 2009, n. 42 in materia di federalismo fiscale e dei relativi decreti legislativi, con particolare riferimento all'art. 26 che prevede, fra l'altro, adeguate forme di reciproca integrazione delle basi informative di cui dispongono le regioni, gli enti locali e lo Stato per le attività di contrasto dell'evasione fiscale;

c) il 14 settembre 2010, presso la Commissione affari costituzionali del Senato, un'audizione sul disegno di legge recante "*Disposizioni in materia di semplificazione dei rapporti della pubblica amministrazione con cittadini e imprese e delega al Governo per l'emanazione della Carta dei doveri delle amministrazioni pubbliche e per la codificazione in materia di pubblica amministrazione*" (AS 2243), il quale contiene diverse norme rilevanti ai fini del diritto alla protezione dei dati personali. Nel corso dell'audizione sono state analizzate le disposizioni di maggior interesse, fornendo, al contempo, specifiche osservazioni e suggerimenti per la riformulazione di alcuni articoli al fine di elevarne lo *standard* di garanzia e di assicurarne la piena conformità ai princìpi e alle regole in materia di protezione dei dati personali. Tali indicazioni –poi compendiate in una segnalazione scritta dell'Autorità alla medesima Commissione– hanno riguardato disposizioni in materia di: semplificazione di misure di sicurezza, in particolare mediante ampliamento dei casi in cui è ammessa la sostituzione del documento programmatico sulla sicurezza con apposita autocertificazione; accesso degli enti previdenziali alla banca dati dei sinistri presso l'ISVAP; elenchi agricoli; riduzione di oneri amministrativi da parte delle autorità indipendenti; *marketing* postale;

d) il 17 marzo 2010, presso la Commissione affari costituzionali della Camera dei deputati, un'audizione nell'ambito dell'indagine conoscitiva sulle autorità amministrative indipendenti avente ad oggetto l'analisi del ruolo e della posizione delle

authority nell'ambito dell'ordinamento italiano. Dopo aver richiamato gli aspetti essenziali caratterizzanti l'Autorità, l'intervento del Garante si è soffermato sulla possibilità di configurare una regolazione uniforme delle autorità indipendenti, oltre che sull'eventuale costituzionalizzazione delle stesse. Sono poi stati oggetto di attenzione l'indipendenza e l'autonomia finanziaria delle autorità, i requisiti, le modalità di nomina e durata dei mandati dei componenti, nonché il sistema di finanziamento.

1.2.2. L'Autorità e le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento

Nel 2010 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 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) interpellanza n. 2-00177, concernente l'invio di *Sms* di propaganda elettorale in occasione della manifestazione di piazza San Giovanni a Roma del 20 marzo 2010. Dopo aver ricevuto diverse segnalazioni, nell'ambito delle attività istruttorie relative alla presunta illecita propaganda elettorale effettuata da diversi partiti per le elezioni regionali del marzo 2010, nei confronti di una società alla quale un partito aveva commissionato l'inoltro di chiamate telefoniche con messaggi preregistrati, l'Autorità ha dichiarato illecito e vietato il trattamento di dati personali correlato all'effettuazione di telefonate preregistrate, per finalità di propaganda elettorale, senza avere documentato l'acquisizione del consenso degli interessati preventivo e informato, ai sensi degli artt. 13, 23 e 130 del Codice (*Nota* 12 dicembre 2010);

b) interrogazione n. 4-07012, in materia di requisiti di legittimazione per il possesso del porto d'armi. L'Autorità ha segnalato che la disciplina in materia di protezione dei dati personali non prevede disposizioni specifiche su eventuali verifiche in ordine alla presenza di fattori di rischio (e in particolare di stress), suscettibili di rappresentare requisiti ostativi al rilascio del porto d'armi. Tuttavia, ogni iniziativa normativa in materia, delle Camere o del Governo, dovrà, ovviamente, tenere conto

dei princìpi –peraltro espressivi di norme comunitarie– sanciti dal Codice, e in particolare dei princìpi di necessità (art. 3), di finalità e di pertinenza (art. 11), nonché (con riferimento ai dati sensibili e giudiziari) di indispensabilità (art. 22) nel trattamento dei dati (*Nota* 22 ottobre 2010);

c) interrogazione n. 4-03022, concernente l'illecito trattamento dei dati delle utenze cellulari riguardanti un militare dell'Arma dei Carabinieri. Al riguardo, l'Autorità ha riferito di aver proceduto all'archiviazione del procedimento dopo che il gestore telefonico, in seguito ad una richiesta di informazioni dell'Ufficio del Garante, aveva dichiarato che non risultavano accessi operati sull'utenza in questione (*Nota* 23 luglio 2010);

d) interrogazione n. 5-02348, concernente la tutela del diritto d'autore in relazione a condotte realizzate attraverso siti *peer to peer*. L'Autorità ha riferito di essere intervenuta nella controversia giudiziale in atto tra la Federazione antipirateria audiovisiva (FAPAV) e la Telecom Italia, con riferimento esclusivo agli aspetti attinenti alla protezione dei dati personali dei soggetti coinvolti, in ragione della funzione di tutela dell'interesse pubblico affidata dalla legge al Garante. In sede giudiziaria si sarebbe dovuto accertare se la FAPAV, attraverso il monitoraggio della rete Internet, avesse illecitamente trattato dati personali consistenti in indirizzi del protocollo *IP* (*Internet protocol*), assegnati a utenti italiani dai rispettivi operatori con conseguente, possibile, inutilizzabilità dei dati (*Nota* 14 aprile 2010). Per ulteriori dettagli si veda il par. 18.5.

1.2.3. L'attività consultiva del Garante sugli atti 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 periodo di riferimento, diversi pareri, i quali hanno riguardato, in particolare:

a) uno schema di decreto dei Ministri dell'interno e delle infrastrutture e dei trasporti concernente le modalità per lo scambio di informazioni tra i suddetti dicasteri ai fini del rilascio e della revoca dei titoli abilitativi alla guida, in attuazione del disposto

di cui all'art. 120, comma 5, del codice della strada (*Parere* 26 gennaio 2011 [doc. *web* n. 1790365]);

b) uno schema di decreto del Ministro della salute concernente l'erogazione, da parte delle farmacie, dell'attività di prenotazione di prestazioni di assistenza specialistica ambulatoriale, di pagamento delle relative quote di partecipazione alla spesa a carico del cittadino e di ritiro di referti relativi a prestazioni di assistenza specialistica ambulatoriale, ai sensi dell'art. 1, comma 2, lett. *f*), del d.lgs. 3 ottobre 2009, n. 153 (*Parere* 19 gennaio 2011 [doc. *web* n. 1784974]);

c) uno schema di deliberazione del Comitato interministeriale per il credito ed il risparmio (CICR), recante attuazione dell'art. 125, comma 1, del d.lgs. 1 settembre 1993, n. 385, e successive modificazioni (Testo unico delle leggi in materia bancaria e creditizia) concernente l'obbligo, per i gestori delle banche dati contenenti informazioni nominative sul credito, di consentire l'accesso a tali banche dati da parte dei finanziatori degli Stati membri dell'Unione europea a condizioni non discriminatorie rispetto a quelle previste per gli altri finanziatori abilitati nel territorio nazionale (*Parere* 16 dicembre 2010 [doc. *web* n. 1779694]);

d) uno schema di decreto del Presidente della Repubblica di modifica e integrazione del d.P.R 28 maggio 2001, n. 284, recante regolamento di attuazione della l. 22 dicembre 1999, n. 512, e concernente il fondo di rotazione per la solidarietà delle vittime dei reati di tipo mafioso (*Parere* 17 novembre 2010 [doc. *web* n. 1779672]);

e) uno di studio di fattibilità e di progettazione operativa della banca dati di cui all'art. 17, comma 1-*bis*, secondo periodo, della l. 3 agosto 1998, n. 269, e successive modificazioni, presentato dal Ministro per le pari opportunità, riguardante la raccolta di tutte le informazioni necessarie per il monitoraggio del fenomeno dell'abuso e dello sfruttamento sessuale dei minori e della pornografia minorile nonché delle azioni di prevenzione e repressione ad esso collegate (*Parere* 22 luglio 2010 [doc. *web* n. 1741941]);

f) uno schema di decreto interministeriale (Ministro dell'interno di concerto con il Ministro delle infrastrutture e dei trasporti, il Ministro dell'economia e delle finanze

e il Ministro per la pubblica amministrazione e l'innovazione) recante l'individuazione delle modalità tecniche ed operative per la comunicazione da parte dei vettori aerei delle informazioni concernenti i passeggeri all'imbarco, di cui all'art. 3 del d.lgs. 2 agosto 2007, n. 144 (*Parere* 22 luglio 2010 [doc. *web* n. 1741930]);

g) uno schema di decreto del Ministro della giustizia, recante regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, ai sensi dell'art. 4, comma 1, del d.l. 29 dicembre 2009, n. 193, convertito dalla l. 22 febbraio 2010, n. 24 (Processo telematico) (*Parere* 15 luglio 2010 [doc. *web* n. 1741725]);

h) uno schema di decreto del Ministro dell'istruzione dell'università e della ricerca, relativo all'Anagrafe nazionale degli studenti (non laureati) istituita dal d.lgs. 4 aprile 2005, n. 76, concernente il trattamento dei dati sui percorsi scolastici, formativi e in apprendistato dei singoli studenti e dei dati relativi alla valutazione degli studenti utili alla prevenzione della dispersione scolastica (*Parere* 16 giugno 2010 [doc. *web* n. 1734404]);

i) uno schema di linee-guida, elaborato dal Gruppo di lavoro tecnico, istituito presso il Ministero dell'interno, relative al programma "tessera del tifoso" (*Parere* 16 giugno 2010 [doc. *web* n. 1733656]);

j) uno schema di decreto del Ministro dell'interno, recante l'istituzione di un registro nazionale delle persone che non hanno fissa dimora (*Parere* 10 giugno 2010 [doc. *web* n. 1741747]);

k) uno schema di decreto del Presidente della Repubblica, concernente il regolamento per l'istituzione e la gestione del Registro pubblico delle opposizioni, previsto, in materia di *marketing* telefonico, dall'art. 130, comma 3-*bis*, del Codice (*Parere* 13 maggio 2010 [doc. *web* n. 1734800]);

l) uno schema di decreto del Ministro dell'istruzione dell'università e della ricerca, recante modalità e contenuti delle prove di ammissione ai corsi di laurea a numero programmato, per l'anno accademico 2010/2011 (*Parere* 6 maggio 2010 [doc. *web* n. 1722452]);

m) uno schema di regolamento interno del Ministero dell'ambiente e della tutela del territorio e del mare, per l'utilizzo della posta elettronica e della rete Internet negli uffici del Ministero (*Parere* 4 marzo 2010 [doc. *web* n. 1706464]);

n) uno schema di decreto del Ministro dell'istruzione dell'università e della ricerca, riguardante le preiscrizioni universitarie per l'anno accademico 2010/2011 (*Parere* 4 marzo 2010 [doc. *web* n. 1706122]);

o) uno schema di decreto del Presidente della Repubblica, recante regolamento di esecuzione del 6° censimento generale dell'agricoltura, emanato ai sensi dell'art. 17, comma 2, del d.l. 25 settembre 2009, n. 135, convertito, con modificazioni, dalla l. 20 novembre 2009, n. 166 (*Parere* 18 febbraio 2010 [doc. *web* n. 1703119]);

p) uno schema di decreto interministeriale (Ministro degli affari esteri di concerto con il Ministro dell'interno), contenente disposizioni per l'attuazione del Sistema di informazione visti (VIS) e lo scambio dei dati fra gli Stati membri dell'Unione europea (*Parere* 28 gennaio 2010 [doc. *web* n. 1694785]);

q) uno schema di decreto del Presidente della Repubblica, recante regolamento per la determinazione dei limiti massimi del trattamento economico onnicomprensivo a carico della finanza pubblica per i rapporti di lavoro dipendente o autonomo (*Parere* 21 gennaio 2010 [doc. *web* n. 1694419]);

r) uno schema di decreto del Ministro per la pubblica amministrazione e l'innovazione, recante modalità di assorbimento della tessera sanitaria nella carta nazionale dei servizi (art. 50, comma 13, d.l. 30 settembre 2003, n. 269, convertito dalla l. 24 novembre 2003, n. 326) (*Parere* 21 gennaio 2010 [doc. *web* n. 1693904]).

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità in relazione a provvedimenti che –ancorché, talvolta, non prevedano specifiche disposizioni in materia di protezione dei dati personali– incidono, in ogni caso, su tale materia. Tra questi provvedimenti si richiamano, in particolare, i seguenti:

a) il decreto del Ministro dell'interno 1° dicembre 2010 (in *G.U.* 14 febbraio 2011, n. 38), recante regolamento sulla disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di vigilanza

e di investigazione privata di cui agli artt. 256-*bis* e 257-*bis* del regolamento di esecuzione del testo unico delle leggi di pubblica sicurezza, nonché dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti;

b) il decreto della Presidenza del Consiglio dei ministri-Dipartimento della gioventù 19 novembre 2010 (in *G.U.* 27 dicembre 2010, n. 30), che destina parte delle risorse di cui all'art. 1, commi 72 e 73, della l. 24 dicembre 2007, n. 247, alle esigenze derivanti dalla peculiare attività lavorativa svolta dai giovani di età inferiore a trentacinque anni;

c) il decreto del Ministro della giustizia 18 ottobre 2010 (in *G.U.* 4 novembre 2010, n. 28), recante regolamento sulla determinazione dei criteri e delle modalità di iscrizione e tenuta del registro degli organismi di mediazione e dell'elenco dei formatori per la mediazione, nonché sull'approvazione delle indennità spettanti agli organismi, ai sensi dell'art. 16 del d.l. 4 marzo 2010, n. 28;

d) il decreto del Ministro del lavoro e delle politiche sociali di concerto con il Ministro per la pubblica amministrazione e l'innovazione 2 novembre 2010 (in *G.U.* 23 novembre 2010, n. 274), recante disposizioni riguardanti il prospetto informativo disabili;

e) il decreto del Ministro dell'istruzione, dell'università e della ricerca di concerto con il Ministro della salute 30 luglio 2010 (in *G.U.* 6 ottobre 2010, n. 234), recante regolamento sulle disposizioni per l'esecuzione delle norme di cui ai commi da 4-*octies* a 4-*decies* dell'art. 1 del d.l. n. 134 del 2009, convertito, con modificazioni, dalla l. n. 167 del 2009, in materia di obblighi per il personale della scuola di documentare i requisiti per avvalersi dei benefici previsti dalla l. 5 febbraio 1992, n. 104, o dalla l. 12 marzo 1999, n. 68;

f) il decreto del Ministro della salute 8 luglio 2010 (in *G.U.* 1 ottobre 2010, n. 230), recante disposizioni per la gestione dell'anagrafe delle imprese di acquacoltura;

g) il decreto del Ministro dell'istruzione, dell'università e della ricerca 4 febbraio 2010 (in *G.U.* 22 aprile 2010, n. 93), recante disciplina delle modalità di iscrizione all'elenco nazionale di fornitori e prestatori di servizi che offrono agevolazioni per gli studenti titolari della Carta dello studente;

h) il decreto del Ministro della salute di concerto con il Ministro del lavoro e delle politiche sociali e il Ministro dell'economia e delle finanze 26 febbraio 2010 (in *G.U.* 19 marzo 2010, n. 65), recante definizione delle modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al Sistema di accoglienza centrale (SAC);

i) l'Intesa tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano del 28 ottobre 2010, adottata ai sensi dell'art. 8, comma 6, della l. 5 giugno 2003, n. 131, sul Piano nazionale di Governo delle liste di attesa per il triennio 2010-2012, di cui all'art. 1, comma 280, della l. 23 dicembre 2005, n. 266 (in *G.U.* 23 novembre 2010, n. 274);

j) il decreto del Ministro dello sviluppo economico 23 marzo 2010 (in *G.U.* 3 aprile 2010, n. 78), recante modifica dei modelli di certificati-tipo inerenti il Registro delle imprese previsti dall'art. 24 del d.P.R. del 7 dicembre 1995, n. 581, e adozione di un modello di ricevuta di accettazione di comunicazione unica per la nascita dell'impresa;

k) il decreto del direttore generale per il mercato, la concorrenza, il consumatore, la vigilanza e la normativa tecnica del Ministero dello sviluppo economico 16 marzo 2010 (in *G.U.* 2 aprile 2010, n. 77), recante approvazione delle integrazioni alle specifiche tecniche per la creazione di programmi informatici finalizzati alla compilazione delle domande e delle denunce da presentare all'Ufficio del Registro delle imprese per via telematica o su supporto informatico, approvate con d.m. 14 agosto 2009, come integrato dal d.m. 24 novembre 2009;

l) il decreto del Presidente della Repubblica 2 agosto 2010 n. 150 (in *G.U.* 10 settembre 2010, n. 212), recante norme relative al rilascio delle informazioni antimafia a seguito degli accessi e accertamenti nei cantieri delle imprese interessate all'esecuzione di lavori pubblici.

1.2.4. Altri pareri

Su espressa richiesta, il Garante ha reso un *parere* sullo schema di decreto legislativo recante modifiche ed integrazioni al d.lgs 7 marzo 2005, n. 82, recante il codice del-

l'amministrazione digitale (CAD), emanato a norma dell'art. 33 della l. 18 giugno 2009, n. 69, con osservazioni che sono state in parte recepite dall'amministrazione proponente (*Parere* 24 giugno 2010 [doc. *web* n. 1737729]).

Il decreto (d.lgs. 30 dicembre 2010, n. 235), fra le varie modifiche apportate al CAD, ridefinisce l'"*autenticazione informatica*" in senso oggettivistico: il riferimento dell'autenticazione, infatti, ora si polarizza sull'oggetto della validazione (il documento informatico) e non più sull'identità (intesa quale insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità) del soggetto che emette il documento. Al riguardo, il Garante ha ritenuto opportuno che, per la nuova definizione in senso oggettivistico del CAD, si ricorresse alla locuzione "*autenticazione del documento informatico*" in luogo di "*autenticazione informatica*"; tale osservazione è stata accolta.

Le novelle apportate al CAD, inoltre, prevedono un incremento della tipologia delle firme, che passano da tre a quattro: firma elettronica, firma elettronica avanzata, firma elettronica qualificata e firma digitale. Al fine di chiarirne l'ambito di utilizzo e scongiurarne un'adozione errata, sia da parte degli utenti, sia da parte delle pp.aa. (con i possibili pregiudizi in ordine al diritto alla protezione dei dati personali), il Garante ha ritenuto opportuno che le regole tecniche da adottare al riguardo non fossero limitate alla sola tipologia di firma digitale (come previsto nello schema di decreto trasmesso per il parere) ma fossero individuate per tutti i tipi di firme. Ed infatti, l'art. 20, comma 3, del CAD, come sostituito dall'art. 13, comma 1, lett. *d*), del decreto, riferisce ora le regole tecniche a "*qualsiasi tipo di firma elettronica avanzata*".

Infine, in ottemperanza alle richieste dell'Autorità, il decreto prevede un maggior coinvolgimento del Garante nella fase di attuazione della riforma, mediante la previsione espressa del *parere* dell'Autorità in relazione a importanti provvedimenti che dovranno essere adottati da DigitPa in materia di consultazione degli indirizzi di posta elettronica certificata ed estrazione di elenchi da parte delle pp.aa. (art. 5, comma 1, lett. *b*), d.lgs. n. 235/2010) e di obbligo per le pp.aa. di definire un adeguato piano di *disaster recovery* (art. 34, comma 2, d.lgs. n. 235/2010).

1.3. LEGGI REGIONALI

Nel corso del 2010 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.

Nella gran parte dei casi sottoposti all'attenzione dell'Autorità (16) è stato riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale rispetto ai profili di protezione dei dati personali.

Solo in 3 casi l'Autorità ha fornito alla Presidenza del Consiglio dei ministri osservazioni in merito alla compatibilità della legge con i princìpi in materia di protezione dei dati personali, ai fini della valutazione in ordine all'eventuale sussistenza dei presupposti necessari all'impugnazione della legge regionale. Si tratta, in particolare, delle seguenti leggi:

a) la legge della Regione Basilicata 23 novembre 2010, n. 32, volta a disciplinare l'anagrafe pubblica degli eletti e degli amministratori. Tale legge, al fine di "*agevolare il diritto di accesso e di informazione*", impone al Consiglio e alla Giunta regionali di rendere disponibili, sui rispettivi siti Internet, taluni dati relativi a ciascun consigliere regionale o componente la Giunta e al presidente della Regione, nonché al Consiglio e alla Giunta regionali. In particolare si sancisce, tra gli altri, l'obbligo di "pubblicazione" integrale della "*dichiarazione dei redditi propri, del coniuge se consenziente, e degli interessi finanziari relativi all'anno precedente l'assunzione*" (art. 3, comma 1, lett. *g*), mentre la legge statale 5 luglio 1982, n. 441 (che disciplina la pubblicità della situazione patrimoniale di titolari di cariche elettive e direttive), prevede la pubblicazione delle sole "*notizie risultanti dal quadro riepilogativo della dichiarazione dei redditi*" (art. 9, comma 1). La modalità di "pubblicazione" prevista dalla legge regionale potrebbe perciò comportare la diffusione di dati non strettamente pertinenti (come, ad es., talune detrazioni fiscali per spese sanitarie o, probabilmente, anche la scelta del contribuente circa la destinazione del "5 per mille") e per giunta in relazione ai soli soggetti cui si riferisce la legge regionale (rispetto a tutti gli altri soggetti che rientrano, invece, nell'ambito di applicazione della l. n. 441/1982),

con possibili ricadute sulla compatibilità della legge con i princìpi costituzionali e con i diritti fondamentali della persona (art. 3 Cost.; artt. 3, 11 e 22, comma 8, del Codice) (*Nota* 29 dicembre 2010);

b) la legge della Regione Calabria 24 settembre 2010, n. 24, recante "*Norme per la pubblicità della situazione patrimoniale dei consiglieri regionali, degli assessori non consiglieri, dei sottosegretari e dei soggetti indicati nell'articolo 15 della legge 5 luglio 1982, n. 441*", che prevede, anch'essa, la pubblicazione integrale delle dichiarazioni dei redditi degli interessati (art. 7, in relazione agli artt. 2, comma 1, 3 e 4, l.r. n. 24/2010), al riguardo l'Autorità ha svolto considerazioni analoghe a quelle da ultimo descritte con riferimento alla legge della Regione Basilicata 23 novembre 2010, n. 32 (*Nota* 8 novembre 2010);

c) la legge della Provincia di Trento 22 aprile 2010, n. 9, recante "*Disposizioni in materia di trasparenza delle informazioni sul lavoro pubblico provinciale. Modificazione della legge sul personale della provincia*". L'art. 1, comma 1, capoverso "Articolo 75-*ter*", attribuisce alla Giunta provinciale la potestà di individuare, con propria "deliberazione", i dati da pubblicare, concernenti, a vario titolo, l'attività delle strutture e del personale dipendente dalle amministrazioni e dagli "*enti strumentali pubblici e privati*". Tra le categorie di dati che la deliberazione dovrà individuare, si prevedono, in particolare, "*i giorni medi di assenza per malattia e per motivi diversi dalle ferie di ciascuna figura professionale o qualifica*". L'Autorità ha rilevato che nella misura in cui tale regime di pubblicità possa riferirsi anche a dati identificativi degli interessati e non, invece, a soli dati anonimi, la norma potrebbe contrastare con il disposto di cui all'art. 22, comma 8, del Codice. Tale ultima norma vieta infatti (nella specie ai soggetti pubblici) di diffondere i dati idonei a rivelare lo stato di salute, quali sono, all'evidenza, i dati relativi alle assenze per malattia (*Nota* 10 maggio 2010).

Di altri profili problematici emersi nell'esame delle leggi regionali si riferisce nel par. 21.6.

2. QUADRO NORMATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

2.1. LE GARANZIE PREVISTE NEL CODICE E ALCUNI RECENTI INTERVENTI MODIFICATIVI

Pur nel sostanziale rispetto del suo impianto generale, il Codice ha subito nel corso del 2010 talune puntuali ma significative modifiche, che di seguito si espongono.

2.1.1. Le modifiche in materia di conoscibilità di notizie relative all'attività del personale addetto a una funzione pubblica

Si è già riferito, nella *Relazione* 2009 (p. 38), dell'approvazione del comma 3-*bis* dell'art. 19 del Codice, relativo all'accessibilità delle notizie riguardanti le prestazioni di chi svolge una funzione pubblica, e delle modifiche all'art. 1 dello stesso Codice.

La norma è contenuta nel disegno di legge sul lavoro pubblico, approvato dalle Camere, rimandato alle stesse dal Presidente della Repubblica e poi divenuto l. n. 183 del 4 novembre 2010 (art. 14, comma 1).

2.1.2. Le modifiche in materia di contrassegni di veicoli di persone invalide

La l. 29 luglio 2010, n. 120, recante disposizioni in materia di circolazione e sicurezza stradale, ha modificato l'art. 74 del Codice sugli aspetti relativi alla disciplina dei contrassegni di veicoli a servizio di persone invalide (art. 58). Il novellato art. 74, comma 1, del Codice, vieta ora l'apposizione, nei contrassegni rilasciati per la circolazione di veicoli a servizio di persone invalide, "*di diciture dalle quali può essere individuata la persona fisica interessata*" e non più di simboli o di altre diciture dai quali possa desumersi la speciale natura del contrassegno. La modifica apportata –in linea con quanto previsto a livello europeo dalla Raccomandazione del Consiglio dell'Unione europea n. 98/376/CE del 4 giugno 1998 con riferimento al modello comunitario unico di contrassegno di parcheggio– consente ora di riportare sul contrassegno anche simboli dai quali possa dedursi la natura dell'agevolazione (ad es., uno specifico disegno) fermo restando che "*le generalità e l'indirizzo della persona fisica interessata sono riportati sui contrassegni con modalità che non consentono la loro diretta visibilità se non in caso di richiesta di esibizione o di necessità di accertamento*".

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

Nel corso del 2010 sono stati approvati alcuni provvedimenti normativi che hanno riguardato il trattamento dei dati personali e l'attività del Garante.

Vanno ricordati, in particolare:

- il d.l. 29 dicembre 2010, n. 225, convertito, con modificazioni, dalla l. 26 febbraio 2011, n. 10, recante "*Proroga di termini previsti da disposizioni legislative e di interventi urgenti in materia tributaria e di sostegno alle imprese e alle famiglie*" (cd. "*milleproroghe*") il quale prevede le seguenti disposizioni normative d'interesse:

  a) l'art. 2, comma 1-*quinquies*, nel prorogare il termine entro il quale l'Istituto superiore di sanità (ISS) deve predisporre la relazione annuale per il Ministro della salute sull'attività delle strutture autorizzate ad applicare le tecniche di procreazione medicalmente assistita (PMA), prevede alcuni delicati flussi informativi. In particolare la norma stabilisce che, fatte salve le disposizioni già vigenti, le predette strutture devono inviare "i dati richiesti" al Ministero della salute che ne cura il successivo invio all'ISS e al Centro nazionale trapianti. Con decreto dello stesso Ministro dovranno essere stabilite le modalità di comunicazione di tali dati dalle strutture autorizzate al Ministero ai fini del successivo inoltro, "*sia in forma aggregata che disaggregata*", ai predetti organismi. Nel corso dei lavori parlamentari, il presidente della Commissione parlamentare di inchiesta sull'efficacia e l'efficienza del Servizio sanitario nazionale ha segnalato al Garante che la non perspicua formulazione della disposizione ("*i dati richiesti*") non lascerebbe intendere agevolmente quale sia il reale contenuto dell'obbligo di comunicazione, comunque riferibile a dati sensibili e di particolare delicatezza quali quelli concernenti le tecniche di procreazione medicalmente assistita. Al riguardo, il Garante, venuto a conoscenza dell'iniziativa normativa e consapevole dei profili problematici della materia, aveva contattato per le vie brevi sia il relatore, sia il Ministro della salute, ricevendo assicurazioni sul fatto che i previsti flussi informativi, dalle strutture autorizzate al Ministero della salute e, da questo, all'Istituto superiore di sanità e al Centro nazionale trapianti, riguardano

Flussi di dati in materia di procreazione assistita

dati anonimi o, comunque, opportunamente codificati, nel rispetto della vigente normativa in materia di protezione dei dati personali. Tale assicurazione è stata fornita, peraltro, dallo stesso relatore nel corso della discussione generale sul provvedimento tenutasi poi al Senato e dal Ministro della salute, nonché dal competente sottosegretario, in diversi comunicati stampa. Lo stesso Ministro, inoltre, ha assicurato che sarà richiesto il *parere* del Garante sullo schema di decreto di attuazione della disposizione normativa, che dovrà stabilire le modalità di comunicazione dei dati; in tale occasione l'Autorità non mancherà di garantire la più ampia collaborazione per la messa a punto di una normativa secondaria rispettosa delle garanzie degli interessati e in particolare del loro anonimato;

Pubblicazione di destinatari di sanzioni

b) l'art. 2, comma 4-*undecies*, modificando l'art. 83-*bis* del d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla l. 6 agosto 2008, n. 133, in materia di sicurezza stradale e regolarità del mercato dell'autotrasporto, stabilisce che possono essere pubblicati sul sito Internet delle autorità competenti le informazioni necessarie per l'identificazione dei destinatari delle sanzioni comminate in caso di violazioni del contratto di trasporto di merci su strada o di ritardato pagamento, ai fini della verifica del rispetto delle sanzioni stesse;

Esercizi pubblici di telefonia e Internet

c) l'art. 2, comma 19, apporta significative modifiche alla disciplina amministrativa degli esercizi pubblici di telefonia e Internet di cui all'art. 7 del d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155, in materia di contrasto al terrorismo (cd. "*decreto Pisanu*"). L'articolo, innanzitutto, proroga "*fino al 31 dicembre 2011*" l'efficacia della norma che obbliga a richiedere la licenza del questore chiunque intenda aprire, quale attività principale, un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni anche telematiche. La proroga riguarda esclusivamente gli Internet point, ossia gli esercizi pubblici che forniscono l'accesso ad Internet in via principale, e non tutte quelle altre attività che mettono a disposizione il collegamento ad Internet quale servizio accessorio. Sono invece abrogati i commi 4

e 5 dell'art. 7 del "*decreto Pisanu*". Ciò comporta che il titolare o il gestore di un esercizio pubblico di telefonia e Internet non è più tenuto ad osservare il monitoraggio delle operazioni svolte dal cliente e l'archiviazione dei relativi dati, nonché le misure di preventiva acquisizione di dati anagrafici riportati su un documento di identità del soggetto;

Archivio dei detenuti

- la l. 26 novembre 2010, n. 199, recante "*Disposizioni relative all'esecuzione presso il domicilio delle pene detentive non superiori ad un anno*", consente ai detenuti di espiare un residuo di pena al di fuori degli istituti penitenziari, e rende disponibile un maggior numero di agenti di polizia penitenziaria per far fronte al *deficit* di organico. Durante i lavori parlamentari al Senato, è stato accolto come raccomandazione un ordine del giorno (G5.100) in base al quale il Governo si impegna, in una seconda fase, a riversare i dati relativi alle amministrazioni penitenziarie e ai detenuti in una banca dati, presso il Ministero della giustizia-Dipartimento dell'amministrazione penitenziaria, costituita da un archivio elettronico, aggiornato ogni sei mesi, "*accessibile, in forme digitali libere e aperte, da parte di chiunque ne abbia interesse attraverso il sito* web *del Ministero della giustizia, secondo le modalità stabilite da apposito regolamento e fatte salve restrizioni dovute a comprovate ragioni di sicurezza*";

Sicurezza urbana

- il d.l. 12 novembre 2010, n. 187, recante "*Misure urgenti in materia di sicurezza*" convertito, con modificazioni, dalla l. 17 dicembre 2010, n. 217, il cui art. 8 in materia di sicurezza urbana, mediante modifiche all'art. 54 del "*Testo unico delle leggi sull'ordinamento degli enti locali*" (d.lgs. 18 agosto 2000, n. 267), prevede che il prefetto, ove le ritenga necessarie, disponga le misure adeguate per assicurare il concorso delle forze di polizia con l'ente locale, nonché "*ispezioni per accertare il regolare svolgimento dei compiti affidati, nonché per l'acquisizione di dati e notizie interessanti altri servizi di carattere generale*";

Legge 4 novembre 2010, n. 183

- la l. 4 novembre 2010, n. 183, in materia di lavoro pubblico e di controversie di lavoro, la quale oltre ad apportare rilevanti modifiche agli artt. 1 e 19 del Codice (richiamate al par. 2.1.1.), ha introdotto diverse disposizioni d'interesse sotto il profilo della protezione dei dati personali, e in particolare:

Trasparenza dei dati relativi ai dirigenti pubblici

a) l'art. 5 della legge integra l'art. 21 della l. 18 giugno 2009, n. 69, che, com'è noto, ha sancito, in capo alle pp.aa., l'obbligo di pubblicare nel proprio sito Internet le retribuzioni annuali, i *curricula vitae*, gli indirizzi di posta elettronica ed i numeri telefonici ad uso professionale dei dirigenti. Al riguardo si rammenta che l'Autorità è stata sentita dal Ministro per la pubblica amministrazione e l'innovazione a suo tempo in ordine alla compatibilità con il diritto alla protezione dei dati personali e, più recentemente, sullo schema di circolare adottato dal predetto Ministro per l'attuazione della norma. In base alla nuova disposizione (art. 21, comma 1-*bis*, l. n. 69/2009), le pp.aa. devono comunicare i predetti dati alla Presidenza del Consiglio dei ministri–Dipartimento della funzione pubblica, per via telematica secondo i criteri e le modalità che saranno individuati con circolare del Ministro per la pubblica amministrazione e l'innovazione, il quale li pubblica nel sito istituzionale del Dipartimento;

Permessi di lavoro per assistenza a portatori di *handicap*

b) l'art. 24 della legge, nell'apportare modifiche alla disciplina dei permessi dal lavoro per l'assistenza a portatori di *handicap* (l. n. 104/1992), istituisce presso la Presidenza del Consiglio dei ministri-Dipartimento della funzione pubblica, una banca dati informatica in cui confluiranno i dati dei dipendenti e delle persone assistite, comunicati da ciascuna amministrazione entro il 31 marzo di ogni anno. La norma prevede che tale banca dati sia istituita e gestita nel rispetto delle misure di sicurezza previste dal Codice, tenendo conto, in particolare, degli specifici accorgimenti previsti, a garanzia degli interessati, nel caso di trattamento di dati sensibili (cifratura dei dati; utilizzo di codici identificativi; conservazione separata dei dati sensibili: art. 22, commi 6 e 7, del Codice). L'art. 24 definisce le predette attività, finalizzate al monitoraggio e alla verifica sulla legittima fruizione dei permessi, "*di rilevante interesse pubblico*" e individua le operazioni di trattamento che possono essere effettuate dalle amministrazioni a tali fini, nonché i termini di conservazione dei dati stessi (2 anni nella banca dati; 30 giorni presso le amministrazioni, allo scopo di organizzarle e comunicarle alla banca dati). La pubblicazione e la divulgazione dei dati e delle relative elaborazioni è consentita solo in forma anonima;

Certificati di malattia

c) l'art. 25 della legge, nel quadro delle misure di controllo sulle assenze dal luogo di lavoro, disciplina l'invio per via telematica dei certificati di malattia dei dipendenti di datori di lavoro privati, dal medico o dalla struttura sanitaria, all'INPS e al datore di lavoro, in termini analoghi a quanto recentemente previsto in ambito pubblico dall'art. 55-*septies* del d.lgs. n. 165/2001, introdotto dall'art. 67, comma 1, del d.lgs. n. 150/2009;

Borsa continua nazionale del lavoro

d) l'art. 48 della legge apporta mirate modifiche al d.lgs. n. 276/2003 in materia di mercato del lavoro e borsa continua nazionale del lavoro, incrementando le informazioni che devono essere ad essa conferite. In particolare, fra i requisiti per l'autorizzazione delle università allo svolgimento dell'attività di intermediazione, è ora previsto anche l'obbligo, per queste ultime, di conferire alla predetta borsa, secondo le modalità previste con decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro dell'istruzione, dell'università e della ricerca, i *curricula* dei propri studenti, che sono resi pubblici anche nei siti Internet dell'ateneo per i dodici mesi successivi alla data di conseguimento del diploma di laurea (art. 6, comma 1, d.lgs. n. 276/2003, come modificato). Viene ampliata la platea dei soggetti autorizzati allo svolgimento dell'attività di intermediazione con riferimento ai "*gestori di siti Internet*", a condizione che svolgano l'attività senza fini di lucro e pubblichino sul sito medesimo i propri dati identificativi. Inoltre, le amministrazioni pubbliche di cui all'art. 1, comma 2, del d.lgs. n. 165/2001, sono tenute a conferire alla borsa continua nazionale del lavoro le informazioni relative alle procedure comparative per il conferimento degli incarichi di collaborazione (art. 7, comma 6-*bis*, d.lgs. n. 165/2001), nonché alle procedure selettive e di avviamento al lavoro (artt. 35 e 36 del d.lgs. n. 165/2001; art. 15 del d.lgs. n. 276/2003, nuovo comma 1-*bis*). Il conferimento dei dati è effettuato anche nel rispetto dei princìpi di trasparenza di cui all'art. 11, comma 3, del d.lgs. n. 150/2009, e con successivo decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro per la pubblica amministrazione e l'innovazione, saranno definite le informazioni da conferire nel rispetto dei princìpi di accessibilità degli atti;

- la l. 13 agosto 2010, n. 136, recante "*Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia*", prevede diverse norme rilevanti ai fini del diritto alla protezione dei dati personali e, in particolare, due deleghe legislative volte alla redazione, l'una, di un codice delle leggi antimafia e delle misure di prevenzione e, l'altra, di un decreto legislativo per la modifica e l'integrazione della disciplina in materia di documentazione antimafia. Al riguardo si segnalano, in particolare, le disposizioni seguenti:

Banca dati della documentazione antimafia

a) l'art. 2, comma 1, indica, tra i princìpi e i criteri direttivi cui il Governo deve attenersi nell'esercizio della delega legislativa in materia di documentazione antimafia, l'istituzione di una banca dati nazionale unica della documentazione antimafia finalizzata all'accelerazione delle procedure di rilascio della medesima documentazione e al potenziamento dell'attività di prevenzione dei tentativi di infiltrazione mafiosa nell'attività d'impresa, cui la Direzione nazionale antimafia può accedere ai fini dell'adempimento delle funzioni di coordinamento di cui all'art. 371-*bis* c.p.p. Si sancisce altresì l'immediata efficacia delle informative antimafia negative su tutto il territorio nazionale con riferimento a tutti i rapporti, anche già in essere, con la p.a.; si prevede altresì la possibilità di integrare la banca dati medesima con dati provenienti dall'estero e secondo modalità di acquisizione da stabilirsi, nonché la possibilità per il procuratore nazionale antimafia di accedere in ogni tempo alla banca dati. Si delega il Governo ad individuare i dati da inserire nella banca dati, i soggetti abilitati a svolgere la raccolta dei medesimi e quelli autorizzati, secondo precise modalità, ad accedervi, con indicazione altresì dei codici di progetto relativi a ciascun lavoro, servizio o fornitura pubblici ovvero ad altri elementi idonei ad identificare la prestazione;

Tracciabilità dei flussi finanziari

b) l'art. 3 sancisce, in capo agli operatori economici coinvolti in appalti pubblici e ai soggetti destinatari di finanziamenti pubblici, l'obbligo (assistito da sanzione amministrativa pecuniaria) di utilizzare, nell'esercizio della loro attività, conti correnti bancari o postali "*dedicati*", al fine di assicurare la tracciabilità dei flussi finanziari, così da prevenire infiltrazioni criminali nell'economia e, in particolare,

nelle concessioni e negli appalti pubblici. Ai medesimi fini la norma prevede altresì che il bonifico bancario o postale debba riportare, in relazione a ciascuna transazione realizzata dai soggetti su elencati, il codice unico di progetto (CUP) relativo all'investimento pubblico sottostante. Gli stessi soggetti sono tenuti a comunicare alla stazione appaltante, oltre agli estremi identificativi dei suddetti conti correnti dedicati, anche le generalità e il codice fiscale delle persone delegate ad operare su di essi. Disposizioni interpretative e attuative delle norme dell'art. 3 della l. n. 136/2010, nonché modifiche alla stessa legge sono contenute nel d.l. 2 novembre 2010, n. 187 (artt. 6 e 7), recante misure urgenti in materia di sicurezza convertito, con modificazioni, dalla l. 17 dicembre 2010, n. 217;

Identificazione degli addetti nei cantieri

c) l'art. 5 reca disposizioni volte ad agevolare l'identificazione degli addetti nei cantieri, integrando il contenuto delle tessere di riconoscimento di cui al d.lgs. 9 aprile 2008, n. 81, con riferimento anche alla data di assunzione nonché, nel caso di subappalto, alla relativa autorizzazione e, nell'ipotesi di lavoratori autonomi, all'indicazione del committente;

Accertamenti fiscali nei confronti di soggetti sottoposti a misure di prevenzione

d) l'art. 7 novella alcune disposizioni della l. 13 settembre 1982, n. 646, in materia di accertamenti fiscali nei confronti di soggetti sottoposti a misure di prevenzione o condannati per taluni reati. Viene in particolare, ampliata la categoria dei soggetti sottoposti alle verifiche e tenuti all'obbligo di comunicare le variazioni nell'entità e nella composizione del patrimonio e si interviene in senso estensivo sull'ambito e sulle finalità degli accertamenti, prevedendo che essi riguardino la verifica, oltre che della posizione fiscale, anche della posizione economica e patrimoniale del soggetto e perseguano il fine di accertare illeciti valutari e societari e comunque in materia economica e finanziaria;

Agenti sotto copertura

e) l'art. 8, comma 4, lett. *b*), nn. 2 e 3, inserisce, all'interno dell'art. 147-*bis* delle norme di attuazione del codice di rito penale, un comma 1-*bis* che estende ai soggetti i quali abbiano operato sotto copertura (ufficiali e agenti di polizia giudiziaria, anche appartenenti ad organismi di polizia esteri, ausiliari e interposte persone) e siano esaminati in dibattimento, le cautele necessarie alla tutela della

"riservatezza" della persona, in ogni caso idonee ad evitare che il volto di tali soggetti sia visibile. La nuova lett. *c-bis*), introdotta nel comma 3, prescrive inoltre la regola del cd. "*esame a distanza*" per chi ha operato sotto copertura. Si segnala che analoga disposizione è introdotta dall'art. 11, comma 2, in relazione all'esame a distanza dei collaboratori di giustizia ammessi al programma provvisorio di protezione o alle misure di protezione, a prescindere dal reato per cui si proceda;

- la l. 29 luglio 2010, n. 120, recante "*Disposizioni in materia di sicurezza stradale*", con la quale il Parlamento ha approvato una significativa riforma del codice della strada. La principale novità d'interesse per l'Autorità è la modifica apportata all'art. 74 del Codice, in materia di contrassegni relativi a veicoli a servizio di persone invalide (art. 58) di cui si è già dato conto nel par. 2.1.2. Si segnalano inoltre le seguenti altre disposizioni in materia di sicurezza e circolazione stradale:

Accertamenti del non uso o abuso di sostanze stupefacenti o alcoliche

a) alcune innovazioni in materia di accertamenti del non uso o abuso di sostanze stupefacenti o alcoliche per i conducenti di veicoli. In particolare:

- si dispone l'effettuazione degli alcool *test* nonché dei *drug test* nei confronti dei neopatentati prima del rilascio della patente. L'estensione delle predette verifiche alla generalità dei conducenti in sede di rinnovo della patente è stato appositamente evitato, perché eccessivamente gravoso; tuttavia, l'obbligo di effettuare i suddetti *test* sussiste per i possessori di patenti professionali al momento del rinnovo (art. 23, comma 1, lett. *c*), che modifica l'art. 119 del d.lgs. 30 aprile 1992, n. 285);
- si rimodulano le procedure per accertare l'eventuale uso di alcool o droghe da parte dei conducenti di veicoli, prevedendo, ad esempio, che quando gli accertamenti forniscono esito positivo ovvero quando si ha altrimenti ragionevole motivo di ritenere che il conducente del veicolo si trovi sotto l'effetto conseguente all'uso di sostanze stupefacenti o psicotrope, i conducenti, nel rispetto della riservatezza personale e senza pregiudizio per l'integrità fisica, possono essere sottoposti ad accertamenti clinico-tossicologici e strumentali ovvero analitici su campioni di mucosa del cavo orale (inizialmente il rife-

rimento era a campioni di liquidi biologici) prelevati a cura di personale sanitario ausiliario delle forze di polizia. Con decreto ministeriale saranno stabilite le modalità di effettuazione degli accertamenti e le caratteristiche degli strumenti da impiegare negli accertamenti medesimi. È altresì previsto che, qualora non sia possibile effettuare il prelievo a cura del personale sanitario ausiliario delle forze di polizia, ovvero qualora il conducente rifiuti di sottoporsi ad esso, gli agenti di polizia stradale accompagnino il conducente presso strutture sanitarie per il prelievo di campioni di liquidi biologici (art. 33, comma 3, lett. *c*) e *d*), che modifica l'art. 187 del d.lgs. n. 285/1992 inserendo il comma 2-*bis*);

- si disciplina la certificazione di assenza di abuso di sostanze alcoliche e di assenza di assunzione di sostanze stupefacenti o psicotrope per chi esercita attività di autotrasporto (art. 50);
- si modifica la disciplina della somministrazione e vendita di alcool nelle ore notturne, prevedendo che i titolari e i gestori dei locali, che proseguano la propria attività oltre le ore 24, devono avere presso almeno un'uscita del locale un apparecchio di rilevazione del tasso alcolemico, di tipo precursore chimico o elettronico, a disposizione dei clienti che desiderino verificare il proprio stato di idoneità alla guida dopo l'assunzione di alcool (art. 54, comma 1);

Casco elettronico e "scatola nera"

b) l'art. 49, relativo all'introduzione del casco elettronico e della cd. "scatola nera", prevede che il Ministro delle infrastrutture e dei trasporti può emanare –sentito per quanto di competenza il Garante– direttive al fine di prevedere, compatibilmente con la normativa comunitaria e nel rispetto della disciplina in materia di protezione dei dati personali, l'impiego in via sperimentale, da parte dei conducenti e degli eventuali passeggeri di ciclomotori e motoveicoli, del casco protettivo elettronico nonché l'equipaggiamento di taluni autoveicoli di grandi dimensioni con un dispositivo elettronico protetto, denominato appunto "scatola nera". Tale dispositivo è idoneo a rilevare, allo scopo di garantire la sicurezza stradale, la

tipologia del percorso, la velocità media e puntuale del veicolo, le condizioni tecnico-meccaniche del medesimo e la condotta di guida, nonché, in caso di incidente, a ricostruirne la dinamica. Al riguardo l'Autorità aveva predisposto una proposta emendativa –inoltrata ai competenti Uffici del Ministero delle infrastrutture e dei trasporti– per demandare la disciplina delle modalità di impiego di tali dispositivi ad un decreto ministeriale da emanarsi sentito il Garante;

c) infine, è stata soppressa, nel corso dell'esame al Senato, una disposizione che imponeva al medico, che fosse venuto a conoscenza di una patologia del suo assistito idonea a scemarne l'idoneità alla guida, di darne tempestiva comunicazione "*...scritta e riservata, nel rispetto delle disposizioni del Codice...*", al Ministero delle infrastrutture e dei trasporti, informando per iscritto l'assistito. Al riguardo, nel testo definitivo approvato l'art. 23, comma 6, che modifica l'art. 128 del codice della strada, prevede che i responsabili delle unità di terapia intensiva o di neurochirurgia sono obbligati a dare comunicazione dei casi di coma di durata superiore a 48 ore agli Uffici provinciali del Dipartimento per i trasporti, la navigazione ed i sistemi informativi e statistici. In seguito a tale comunicazione i soggetti di cui al periodo precedente sono tenuti alla revisione della patente di guida;

Sistema informatico dei flussi informativi relativi ai mercati dell'energia elettrica e del gas

- il d.l. 8 luglio 2010, n. 105, convertito, con modificazioni, dalla l. 13 agosto 2010, n. 129, recante "*Misure urgenti in materia di energia*", che, al fine di sostenere la competitività e di incentivare la migliore funzionalità delle attività delle imprese operanti nel settore dell'energia elettrica e del gas naturale, istituisce, presso l'Acquirente unico S.p.A., un Sistema informatico integrato per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica e del gas, basato su di una banca dati dei punti di prelievo e dei dati identificativi dei clienti finali (art. 1-*bis*). Al riguardo, il comma 3 del predetto art. 1-*bis* attribuisce all'Autorità per l'energia elettrica e il gas il potere di adottare "*nel rispetto delle norme stabilite dal Garante per la protezione dei dati personali ... specifici criteri e modalità per il trattamento dei dati personali e sensibili*" nell'ambito del citato Sistema informatico. La formulazione

della norma deriva dall'approvazione di un emendamento parlamentare al disegno di legge volto, secondo il proponente, a "*specificare meglio il ruolo del Garante per la protezione dei dati personali*" nell'ambito di tale disposizione. La formulazione originaria della norma prevedeva, invece, che l'Autorità per l'energia elettrica e il gas stabilisse i criteri e le modalità per il trattamento dei dati personali e sensibili "*sentito il Garante*". Al riguardo, è in corso una specifica collaborazione tra il Garante e la predetta Autorità ai fini dell'attuazione del disposto normativo e dell'adozione dei criteri in questione;

- la l. 4 giugno 2010, n. 96, recante "*Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2009*", prevede talune norme rilevanti ai fini del diritto alla protezione dei dati personali, di seguito illustrate:

  a) l'art. 13 nell'inserire nell'art. 33, comma 1, della l. 7 luglio 2009, n. 88, (Legge comunitaria 2008, le lettere da *d-bis* a *d-quinquies*), integra i princìpi e i criteri direttivi cui il Governo dovrà attenersi nell'esercizio della delega ivi prevista, volta ad attuare la Direttiva n. 2004/48/CE relativa ai contratti di credito ai consumatori e a prevedere modifiche e integrazioni alla disciplina relativa ai soggetti operanti nel settore finanziario, ai mediatori creditizi ed agli agenti in attività finanziaria. La novella, alla lett. *d-ter*) attribuisce al Governo il compito di istituire "*nel rispetto della disciplina in materia di tutela della riservatezza dei dati personali*", un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al fenomeno dei furti d'identità. Il sistema è basato su un archivio centrale informatizzato, istituito nell'ambito del Ministero dell'economia e delle finanze, titolare dell'archivio medesimo e del connesso trattamento dei dati. Secondo quanto previsto dall'art. 29 del Codice, il Ministero designa per la gestione dell'archivio e in qualità di responsabile del trattamento dei dati personali la società CONSAP S.p.A. Con tale previsione normativa si è demandato al Governo di disciplinare la materia, malgrado il Senato avesse già approvato, al riguardo, un disegno di legge

Sistema pubblico di prevenzione delle frodi nel settore del credito al consumo

(AS 414-Costa e AS 507-Barbolini), successivamente esaminato dalla Commissione finanze della Camera (AC 2699). Recentemente il Governo ha predisposto lo schema di decreto legislativo previsto dalla legge comunitaria, riproducendo sostanzialmente il testo all'esame della Camera sul quale il Garante ha espresso forti perplessità nel corso di un'audizione tenuta presso la Commissione finanze della medesima Camera il 25 novembre 2009. In tale occasione, l'Autorità, nel rilevare che il testo non corrispondeva del tutto alle indicazioni fornite in una precedente audizione del luglio del 2008 presso l'omologa commissione del Senato, ha evidenziato uno "*snaturamento*" dell'originario impianto normativo e della configurazione del sistema, il quale, diversamente da quanto originariamente prospettato, non è più solo uno "*snodo tecnico*" attraverso il quale il gestore provvede a riscontrare le richieste di verifica provenienti dai soggetti aderenti al sistema su dati e informazioni registrati in altre, distinte banche dati, ma assume, esso stesso, seppure in parte, natura di vero e proprio archivio. Infatti, l'"*archivio*" sarebbe composto anche da un "*modulo informatico di allerta*" nel quale sarebbero memorizzate le informazioni trasmesse dagli aderenti relative: a) alle frodi subite; b) ai casi che configurano un rischio di frodi; c) alle allerta preventive trasmesse dal titolare dell'archivio agli aderenti. Tali informazioni, peraltro, sarebbero conservate nell'archivio per il tempo necessario agli aderenti per accertare l'effettiva sussistenza del rischio di frodi (art. 30-*quater*, comma 1, lett. *c*), del d. lgs n. 141/2010, inserito dall'art. 1 dello schema di decreto). La previsione di tali flussi informativi è destinata a creare una banca dati di notevoli dimensioni, contenente informazioni di particolare delicatezza. Essa rischia, peraltro, di incoraggiare pericolose stigmatizzazioni dei cittadini che ricorrono al credito o ad altri servizi, sulla base di una valutazione rimessa agli stessi operatori del settore e non alle pubbliche autorità competenti in materia di prevenzione e repressione di comportamenti fraudolenti. Analoghe, forti perplessità suscita, poi, la previsione di un servizio volto a ricevere segnalazioni da parte di soggetti che hanno subito o temono di aver subito frodi configuranti ipotesi di furto di

identità (art. 30-*ter*, comma 8, del d.lgs. n. 141/2010, inserito dall'art. 1 dello schema). Lo schema di decreto legislativo estende, poi, la "partecipazione" al sistema a nuove categorie di soggetti, per finalità, peraltro, non sempre ben identificate o certamente molto diverse da quelle del credito al consumo (ad es., "*gestori di sistemi di informazioni creditizie*", nonché forze di polizia). Infine, contrariamente a quanto richiesto dal Garante, lo schema di decreto prevede che ulteriori flussi di dati idonei a perseguire le finalità di contrasto delle frodi potranno essere individuati con il previsto decreto ministeriale di attuazione (art. 30-*quinquies*, comma 3, del d.lgs. n. 141/2010, inserito dall'art. 1 dello schema). La lett. *d-quater*) del comma 1, dell'art. 33 inserisce inoltre, tra i princìpi e criteri direttivi, la previsione secondo cui il diniego del finanziamento da parte dei soggetti abilitati all'esercizio dell'attività di erogazione di credito ai consumatori sia obbligatoriamente motivato, intendendosi la motivazione non integrata nel caso di mero rinvio all'esito della consultazione di banche di dati e di sistemi di informazione creditizia. Infine, la lett. *d-quinquies*) prevede, quale ulteriore criterio di delega, la previsione secondo cui al soggetto richiedente cui venga negato il finanziamento sia consentito di prendere visione e di estrarre copia, a sue spese, del provvedimento di diniego e della rispettiva motivazione;

Pubblicità dei compensi per i "*manager*"

b) l'art. 24 prevede forme di pubblicità dei compensi corrisposti ai "*manager*" delle società quotate;

Lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti

c) l'art. 54, nel delegare il Governo ad adottare il d.lgs. recante le norme occorrenti per dare attuazione alla Decisione quadro n. 2001/413/GAI del Consiglio, del 28 maggio 2001, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, prevede, quale specifico e ulteriore principio e criterio direttivo, l'introduzione, nel Titolo V del d.lgs. 21 novembre 2007, n. 231, di due nuove fattispecie criminose. La prima dovrà sanzionare con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro la condotta di chi fabbrica, acquista, detiene o aliena strumenti, articoli, programmi informatici e ogni altro mezzo destinato esclusivamente alla contraffazione o alla

falsificazione di strumenti di pagamento diversi dai contanti, del tipo di quelli indicati nell'art. 55 del medesimo d.lgs. n. 231/2007 (carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi). La seconda dovrà punire con la reclusione da uno a tre anni e con la multa da 200 a 1.000 euro la condotta di chi fabbrica, acquista, detiene o aliena programmi informatici destinati esclusivamente al trasferimento di denaro o di altri valori monetari, allo scopo di procurare a sé o ad altri un indebito vantaggio economico, mediante l'introduzione, la variazione o la soppressione non autorizzata di dati elettronici, in particolare di dati personali, oppure mediante un'interferenza non autorizzata con il funzionamento del programma o del sistema elettronico;

- il d.l. 31 maggio 2010, n. 78, recante misure urgenti in materia di stabilizzazione finanziaria e di competitività economica convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122 e in particolare:

Modernizzazione dei pagamenti effettuati dalle pp.aa.

a) l'art. 4, al fine di assicurare ulteriore efficienza nei pagamenti e nei rimborsi dei tributi effettuati da parte di enti e pp.aa. a cittadini e utenti, prevede che il Ministero dell'economia e delle finanze promuova la realizzazione di un servizio nazionale per pagamenti su carte elettroniche istituzionali, inclusa la tessera sanitaria. A tal fine, il Ministero, con propri provvedimenti, dovrà individuare, fra l'altro, gli *standard* tecnici del servizio di pagamento e le modalità con cui i soggetti pubblici distributori di carte elettroniche istituzionali potranno avvalersene;

Controllo della spesa sanitaria

b) l'art. 11 prevede, al comma 15 che, nelle more dell'emanazione dei decreti attuativi del comma 13, dell'art. 50 del d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. 24 novembre 2003, n. 326, ai fini dell'evoluzione della tessera sanitaria (TS) verso la tessera sanitaria-carta nazionale dei servizi (TS-CNS), in occasione del rinnovo delle tessere in scadenza il Ministero dell'economia e delle finanze curi la generazione e la progressiva consegna della TS-CNS. Il comma 16 del medesimo art. 11 prevede, poi, che nelle more dell'emanazione dei decreti attuativi di cui al comma 5-*bis*, ultimo periodo, del

medesimo art. 50, al fine di accelerare il conseguimento dei risparmi derivanti dall'adozione delle modalità telematiche per la trasmissione delle ricette mediche (art. 50, commi 4, 5 e 5-*bis*, d.l. n. 269/2003), il Ministero dell'economia e delle finanze curi l'avvio della diffusione della suddetta procedura telematica, adottando, in quanto compatibili, le modalità tecniche operative di cui all'Allegato 1 del decreto del Ministro della salute del 26 febbraio 2010, recante modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al Sistema di accoglienza centrale (SAC). L'invio telematico dei predetti dati sostituisce a tutti gli effetti la prescrizione medica in formato cartaceo;

Casellario dell'assistenza

c) l'art. 13 prevede l'istituzione presso l'Istituto nazionale della previdenza sociale, del Casellario dell'assistenza per la raccolta, la conservazione e la gestione dei dati, dei redditi e di altre informazioni relativi ai soggetti aventi titolo alle prestazioni di natura assistenziale. Il Casellario costituisce l'anagrafe generale delle posizioni assistenziali e delle relative prestazioni, condivisa tra tutte le amministrazioni centrali dello Stato, gli enti locali, le organizzazioni *no profit* e gli organismi gestori di forme di previdenza e assistenza obbligatorie che devono fornire i dati e le informazioni contenute nei propri archivi e banche dati, per la realizzazione di una base conoscitiva utile ad una migliore gestione della rete dell'assistenza sociale. L'utilizzo dei dati e delle informazioni del Casellario dovrà avvenire nel rispetto della normativa sulla protezione dei dati personali. Gli enti, le amministrazioni e i soggetti interessati dovranno trasmettere obbligatoriamente, in via telematica, al Casellario i dati e le informazioni relativi a tutte le posizioni risultanti nei propri archivi e banche dati secondo criteri e modalità di trasmissione stabilite dall'INPS. Con decreto del Ministro del lavoro e delle politiche sociali saranno disciplinate le modalità di attuazione del *database*;

Partecipazione dei comuni all'attività di accertamento fiscale e contributivo

d) l'art. 18 potenzia la partecipazione dei comuni all'accertamento fiscale e contributivo, mediante mirate modifiche, in particolare, agli artt. 44 del d.P.R n. 600/1973 e 1 del d.l. 30 settembre 2005, n. 203, convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248, che incrementano l'accesso dei comuni a dati

utili a tali fini e, in particolare, alle dichiarazioni dei redditi. La partecipazione consiste, tra l'altro, nella segnalazione all'Agenzia delle entrate, alla Guardia di finanza e all'INPS di elementi utili ad integrare i dati contenuti nelle dichiarazioni presentate dai contribuenti, per la determinazione di maggiori imponibili fiscali e contributivi. A tali fini l'Agenzia delle entrate mette a disposizione dei comuni le dichiarazioni dei contribuenti in essi residenti; il comune di domicilio fiscale del contribuente comunica ogni elemento in suo possesso utile alla determinazione del reddito complessivo. Con provvedimento del direttore dell'Agenzia delle entrate, d'intesa con l'INPS e la Conferenza unificata, sono stabilite le modalità tecniche di accesso alle banche dati e di trasmissione ai comuni, anche in via telematica, di copia delle dichiarazioni relative ai contribuenti in essi residenti, nonché quelle della partecipazione dei comuni all'accertamento fiscale e contributivo, anche attraverso enti che, partecipati dai comuni stessi, dovranno garantire ad essi l'accesso alle banche dati utilizzate;

Aggiornamento del catasto

e) l'art. 19 prevede che a decorrere dal 1° gennaio 2011, è attivata l'Anagrafe immobiliare integrata, costituita e gestita dall'Agenzia del territorio. L'Anagrafe immobiliare integrata attesta, ai fini fiscali, lo stato di integrazione delle banche dati disponibili presso l'Agenzia del territorio per ciascun immobile, individuandone il soggetto titolare di diritti reali. In fase di prima applicazione, l'accesso all'Anagrafe immobiliare integrata è garantito ai comuni sulla base di un sistema di regole tecnico-giuridiche, emanate con uno o più decreti del Ministro dell'economia e delle finanze, previa intesa con la Conferenza Stato-città ed autonomie locali. I decreti devono assicurare comunque ai comuni la piena accessibilità ed interoperabilità applicativa delle banche dati con l'Agenzia del territorio, relativamente ai dati catastali, anche al fine di contribuire al miglioramento ed aggiornamento della qualità dei dati, secondo le specifiche tecniche e le modalità operative stabilite con i medesimi decreti. La consultazione delle banche dati del catasto terreni (censuaria e cartografica), del catasto edilizio urbano, nonché dei dati di superficie delle unità immobiliari urbane a destinazione ordinaria, è

garantita ai comuni su tutto il territorio nazionale, ad esclusione delle Province autonome di Trento e Bolzano, attraverso il Sistema telematico, il Portale per i comuni ed il Sistema di interscambio, gestiti dall'Agenzia del territorio. Per assicurare l'unitarietà del sistema informativo catastale nazionale e, in attuazione dei princìpi di accessibilità ed interoperabilità applicativa delle banche dati, i comuni utilizzano le applicazioni informatiche e i sistemi di interscambio messi a disposizione dall'Agenzia del territorio, anche al fine di contribuire al miglioramento dei dati catastali. Sono in ogni caso conservate in capo allo Stato ed esercitate dall'Agenzia del territorio le funzioni in materia, fra l'altro, di controllo della qualità delle informazioni catastali e dei processi di aggiornamento degli atti, di gestione unitaria e certificata della base dei dati catastali e dei flussi di aggiornamento delle informazioni, assicurando il coordinamento operativo per la loro utilizzazione ai fini istituzionali attraverso il sistema pubblico di connettività e garantendo l'accesso ai dati a tutti i soggetti interessati, nonché di gestione dell'Anagrafe immobiliare integrata;

Aggiornamento dell'accertamento sintetico

f) l'art. 22 rivisita le disposizioni per l'accertamento sintetico dei redditi, al fine di adeguarlo al contesto socio-economico attuale, mutato nel corso dell'ultimo decennio, rendendolo più efficiente e dotandolo di garanzie per il contribuente, anche mediante il contraddittorio. L'Ufficio competente può sempre determinare sinteticamente il reddito complessivo del contribuente sulla base delle spese di qualsiasi genere sostenute nel corso del periodo d'imposta, salva la prova che il relativo finanziamento è avvenuto con redditi diversi da quelli posseduti nello stesso periodo d'imposta. La determinazione sintetica può essere altresì fondata sul contenuto induttivo di elementi indicativi di capacità contributiva individuato mediante l'analisi di campioni significativi di contribuenti, differenziati anche in funzione del nucleo familiare e dell'area territoriale di appartenenza. L'ufficio che procede alla determinazione sintetica del reddito complessivo ha l'obbligo di invitare il contribuente a comparire di persona o per mezzo di rappresentanti per fornire dati e notizie rilevanti ai fini dell'accertamento;

Incrocio tra le basi dati dell'INPS e dell'Agenzia delle entrate per contrastare la microevasione diffusa

g) l'art. 28 stabilisce che al fine di contrastare l'inadempimento dell'obbligo di presentazione della dichiarazione dei redditi, l'Agenzia delle entrate potrà eseguire specifici controlli sulle posizioni dei soggetti che risultano aver percepito e non dichiarato redditi di lavoro dipendente ed assimilati sui quali, in base ai flussi informativi dell'INPS, risultano versati i contributi previdenziali e non risultano effettuate le previste ritenute. Anche a tal fine le attività di controllo e di accertamento realizzabili con modalità automatizzate sono incrementate e rese più efficaci attribuendone la effettuazione ad apposite articolazioni dell'Agenzia delle entrate;

Prestazioni sociali agevolate

h) l'art. 38 prevede, al comma 1, che gli enti che erogano prestazioni sociali agevolate, comprese quelle relative al diritto allo studio universitario, a seguito di presentazione della dichiarazione sostitutiva unica di cui all'art. 4 del d.lgs. 31 marzo 1998, n. 109, comunicano all'INPS, nel rispetto del Codice e nei termini e con modalità telematiche previste dall'Istituto medesimo sulla base di direttive del Ministero del lavoro e delle politiche sociali, i dati dei beneficiari delle prestazioni agevolate. Le informazioni raccolte sono trasmesse in forma anonima anche al Ministero del lavoro e delle politiche sociali ai fini dell'alimentazione del Sistema informativo dei servizi sociali, di cui all'art. 21 della l. 8 novembre 2000, n. 328. In base al comma 2, con apposita convenzione stipulata tra l'INPS e l'Agenzia delle entrate, nel rispetto delle disposizioni del Codice, sono disciplinate le modalità attuative e le specifiche tecniche per lo scambio delle informazioni necessarie all'emersione dei soggetti che in ragione del maggior reddito accertato in via definitiva non avrebbero potuto fruire o avrebbero fruito in misura inferiore delle prestazioni sociali agevolate di cui al comma 1.

Codice fiscale

Il comma 6 stabilisce che data la valenza del codice fiscale quale elemento identificativo di ogni soggetto, da indicare in ogni atto relativo a rapporti intercorrenti con la p.a., l'amministrazione finanziaria rende disponibile a chiunque, con servizio di libero accesso, la possibilità di verificare, mediante i dati disponibili in Anagrafe tributaria, l'esistenza e la corrispondenza tra il codice fiscale e i dati

anagrafici inseriti. Tenuto inoltre conto che i rapporti tra pp.aa., nonché quelli intercorrenti tra queste e altri soggetti pubblici o privati, devono essere tenuti sulla base del codice fiscale, per favorire la qualità delle informazioni presso la p.a. e nelle more della completa attivazione dell'indice delle anagrafi INA-SAIA, l'amministrazione finanziaria rende accessibili alle pp.aa., alle società interamente partecipate da enti pubblici o con prevalente capitale pubblico, ai concessionari e gestori di pubblici servizi ed, infine, ai privati che cooperano con le attività dell'amministrazione finanziaria, il codice fiscale registrato nell'Anagrafe tributaria ed i dati anagrafici ad esso correlati, al fine di verificarne l'esistenza e la corrispondenza, oltre che consentire l'acquisizione delle corrette informazioni ove mancanti. Tali informazioni sono rese disponibili, previa stipula di apposita convenzione, anche con le modalità della cooperazione applicativa;

Censimento

i) l'art. 50 indìce il 15° censimento generale della popolazione e delle abitazioni, di cui al regolamento 9 luglio 2008, n. 763, del Parlamento europeo e del Consiglio, nonché il 9° censimento generale dell'industria e dei servizi ed il censimento delle istituzioni *no profit*. Ai sensi del d.lgs. n. 322/89 l'ISTAT organizza le operazioni di ciascun censimento attraverso il Piano generale di censimento stabilendo, fra l'altro, i soggetti tenuti all'obbligo di risposta, il trattamento dei dati e la tutela della riservatezza, le modalità di diffusione dei dati, anche con frequenza inferiore alle tre unità, ad esclusione dei dati di cui all'art. 22 del Codice (dati sensibili e giudiziari). Con apposite circolari e nel rispetto della riservatezza, l'ISTAT stabilisce la tipologia ed il formato dei dati individuali nominativi dell'Anagrafe della popolazione residente, utili per le operazioni censuarie, che i comuni devono fornire all'ISTAT. Il Ministero dell'interno vigila sulla corretta osservanza da parte dei comuni dei loro obblighi di comunicazione. Anche a tal fine, a modifica della normativa istitutiva dell'INA (Indice nazionale delle anagrafi), l'art. 1, comma 6, della l. 24 dicembre 1954, n. 1228, è sostituito dal seguente: "*6. L'INA promuove la circolarità delle informazioni anagrafiche essenziali al fine di consentire alle amministrazioni pubbliche centrali e locali collegate*

la disponibilità, in tempo reale, dei dati relativi alle generalità, alla cittadinanza, alla famiglia anagrafica nonché all'indirizzo anagrafico delle persone residenti in Italia, certificati dai comuni e, limitatamente al codice fiscale, dall'Agenzia delle entrate". Conseguentemente, con decreto (da adottare ai sensi dell'art. 1, comma 7, della predetta l. n. 1228/1954), saranno emanate le disposizioni volte ad armonizzare il regolamento di gestione dell'INA con quanto previsto dal citato comma;

Consenso o diniego alle donazioni di organi

- il d.l. 30 dicembre 2009, n. 194, recante "*Proroga di termini previsti da disposizioni legislative*", convertito, con modificazioni, dalla l. 26 febbraio 2010, n. 25, il cui art. 3, comma 8-*bis*, nel novellare l'art. 3 del testo unico delle leggi di pubblica sicurezza, ha previsto che la carta d'identità può altresì contenere l'indicazione del consenso ovvero del diniego a donare i propri organi in caso di morte;

Processo telematico

- il d.l. 29 dicembre 2009, n. 193, recante "*Interventi urgenti in materia di funzionalità del sistema giudiziario*", convertito, con modificazioni, dalla l. 22 febbraio 2010, n. 24, il cui art. 4 demanda a uno o più decreti del Ministro della giustizia –di concerto con il Ministro per la pubblica amministrazione e l'innovazione, sentiti DigitPa (già Cnipa) e il Garante– l'individuazione delle regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei princìpi previsti dal Codice dell'amministrazione digitale (v. Relazione 2009, p. 45 ss.).

Sono stati infine adottati alcuni decreti legislativi d'interesse in materia di protezione dei dati personali, tra i quali si richiamano, in particolare:

Certificazione dei macchinisti

- il d.lgs. 30 dicembre 2010, n. 247, concernente l'attuazione della Direttiva n. 2007/59/CE relativa alla certificazione dei macchinisti addetti alla guida di locomotori e treni sul sistema ferroviario della Comunità. Il decreto prevede che ciascun macchinista deve avere l'idoneità e le qualifiche necessarie per assicurare la condotta di treni e deve possedere apposita licenza (che attesti che il macchinista soddisfa le condizioni minime per quanto riguarda i requisiti medici, la formazione scolastica di base e la competenza professionale generale) e uno o più certificati, che indicano

le infrastrutture sulle quali il titolare è autorizzato a circolare ed i veicoli che il titolare è autorizzato a condurre. Il decreto, dopo aver previsto l'istituzione di un sistema di monitoraggio dei macchinisti da parte delle imprese ferroviarie e dei gestori dell'infrastruttura (art. 17), stabilisce che l'Agenzia nazionale per la sicurezza delle ferrovie, i gestori dell'infrastruttura e le imprese ferroviarie si accertino che i registri da essi istituiti (registro delle licenze di conduzione treni e registri dei certificati) e le modalità di utilizzo di tali registri rispettino le disposizioni del Codice (art. 19). I macchinisti hanno accesso ai propri dati conservati nel registro dell'Agenzia ed in quelli delle imprese ferroviarie o dei gestori delle infrastrutture e ne ottengono copia su richiesta;

Codice dell'amministrazione digitale

- il d.lgs. 30 dicembre 2010, n. 235, concernente modifiche ed integrazioni al d.lgs. n. 82/2005, Codice dell'amministrazione digitale (CAD), sul cui schema il Garante ha espresso *parere* (cfr. par. 1.2.4.). Il decreto prevede significative innovazioni al CAD volte a garantire la digitalizzazione dei procedimenti amministrativi rispetto a un panorama tecnologico in evoluzione. Le principali novità riguardano la validità dei documenti informatici, la conservazione digitale dei documenti, la posta elettronica certificata, la trasmissione delle informazioni via *web*, l'accesso ai servizi in rete, le firme elettroniche, il protocollo informatico e il fascicolo elettronico, la sicurezza digitale. Di particolare rilevanza, sotto il profilo della protezione dei dati personali, risulta il novellato art. 54 del CAD che arricchisce il contenuto dei siti istituzionali delle pp.aa. a fini di trasparenza, prevedendo che sugli stessi siano pubblicati, in modo integrale, anche tutti i bandi di concorso. La norma obbliga poi le pp.aa. a comunicare parte degli stessi dati al Dipartimento della funzione pubblica, per la successiva pubblicazione anche sul sito del Dipartimento stesso (art. 54, comma 1-*bis*). Infine, il nuovo art. 60 del CAD individua espressamente alcune "*basi di dati di interesse nazionale*" la cui conoscenza è utilizzabile dalle pp.aa., anche per fini statistici, per l'esercizio delle proprie funzioni nel rispetto delle norme vigenti, e in particolare: il repertorio nazionale dei dati territoriali, l'indice nazionale delle anagrafi, la banca dati nazionale dei contratti pubblici, il casellario giudiziale, il registro delle

imprese e gli archivi automatizzati in materia di immigrazione e di asilo di cui all'art. 2, comma 2, del d.P.R. n. 242/2004;

Controlli in materia di armi

- il d.lgs. 26 ottobre 2010, n. 204, recante attuazione della Direttiva n. 2008/51/CE, relativa al controllo dell'acquisizione e della detenzione di armi, che entrerà in vigore il 1 luglio 2011. In particolare, esso prevede, modificando l'art. 35 del testo unico delle leggi di pubblica sicurezza, l'obbligo di un apposito registro delle operazioni giornaliere tenuto in formato elettronico a carico degli armaioli, da conservare per un periodo di cinquanta anni; è altresì previsto a carico degli stessi un obbligo informativo mensile all'Ufficio di polizia competente per territorio. Al termine dell'attività i registri sono consegnati all'autorità di pubblica sicurezza, responsabile della conservazione per il periodo necessario. Le informazioni registrate nel sistema informatico di raccolta dei dati del Ministero dell'interno di cui al d.lgs. n. 8/2010 sono conservate per i cinquanta anni successivi al termine dell'attività. Il predetto sistema consente al Ministero dell'interno l'identificazione univoca e la tracciabilità delle armi lungo tutta la catena della fornitura. Nel novellare il predetto art. 35, inoltre, il d.lgs conferma l'attuale previsione che subordina il rilascio del nulla osta all'acquisto di armi da parte del questore all'assenza di malattie mentali o di altri vizi che diminuiscano anche temporaneamente la capacità di intendere e di volere del richiedente; include poi, tra i requisiti ostativi al rilascio del nulla osta, anche l'assunzione, da parte del richiedente, ed ancorché occasionale, di sostanze stupefacenti o psicotrope, nonché l'abuso di alcool, prevedendo altresì la presentazione di "ogni altra" (rispetto al certificato medico-legale di cui all'attuale norma) certificazione sanitaria prevista dalle disposizioni vigenti. Si richiama l'attenzione in particolare sul comma 10 del nuovo art. 35 ai sensi del quale, tanto il provvedimento di rilascio del nulla osta quanto quello della licenza di porto d'armi, devono essere comunicati dall'interessato ai conviventi maggiorenni, anche diversi dai familiari, compreso il convivente *more uxorio*, individuati dal regolamento di attuazione e indicati dallo stesso interessato all'atto dell'istanza. Si segnala infine che l'art. 6 del decreto legislativo demanda ad un successivo decreto interministeriale dei Ministri della salute

e dell'interno –sul cui schema sarà acquisito il *parere* del Garante– la previsione delle modalità con le quali effettuare lo scambio protetto dei dati informatizzati tra il Servizio sanitario nazionale e gli Uffici delle forze dell'ordine nei procedimenti finalizzati all'acquisizione, alla detenzione e al conseguimento di qualunque licenza di porto d'armi e ad un decreto del Ministro dell'interno la disciplina delle modalità di funzionamento e di utilizzazione del sistema informatico di raccolta dei dati relativi alle armi ed alle munizioni in relazione alla tracciabilità delle stesse;

Verifica del merito creditizio

- il d.lgs. 13 agosto 2010, n. 141, recante attuazione della Direttiva n. 2008/48/CE relativa ai contratti di credito ai consumatori, nonché modifiche al testo unico bancario in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi, adottato in attuazione dell'art. 33 della l. n. 88/2009 (Legge comunitaria 2008). Il decreto non ha disciplinato gli aspetti, pur previsti nella legge delega, concernenti il contrasto delle frodi nel settore del credito al consumo, con particolare riferimento al fenomeno dei furti d'identità (v. par. 2.2.). Tuttavia esso reca disposizioni rilevanti ai fini del diritto alla protezione dei dati personali, in particolare nel Titolo I che apporta, all'art. 1, talune modifiche al testo unico bancario (d.lgs.1 settembre 1993, n. 385): nel dettaglio, l'art. 124-*bis* (*Verifica del merito creditizio*) prevede prima della conclusione del contratto di credito, una valutazione del merito creditizio del consumatore ad opera del finanziatore sulla base di informazioni adeguate fornite dal consumatore stesso o ottenute consultando una banca dati pertinente; l'art. 125 (*Banche dati*) prevede che i gestori delle banche dati contenenti informazioni nominative sul credito debbano consentire l'accesso dei finanziatori degli Stati membri dell'Unione europea alle proprie banche dati a condizioni non discriminatorie rispetto a quelle previste per i finanziatori operanti nel territorio nazionale. Al riguardo, spetta al CICR (Comitato interministeriale per il credito ed il risparmio), sentito il Garante, individuare le condizioni di accesso alle banche dati (v. par. 1.2.3., sul *parere* del Garante sullo schema di delibera del CICR);

Atto notarile informatico

- il d.lgs. 2 luglio 2010, n. 110, recante "*Disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'art. 65 della legge 18 giugno 2009, n. 69*".

Di specifico interesse per l'Autorità è l'art. 62-*bis* della l. n. 89/1913, introdotto dall'art. 1 del decreto legislativo in questione, il quale prevede che il notaio per la conservazione degli atti (di cui agli artt. 61 e 72, comma 3, della legge), se informatici, si avvale della struttura predisposta e gestita dal Consiglio nazionale del notariato nel rispetto dei princìpi di cui all'art. 60 del CAD (d.lgs. 7 marzo 2005, n. 82). Gli atti conservati nella suddetta struttura costituiscono ad ogni effetto di legge originali informatici da cui possono essere tratti duplicati e copie. Il Consiglio nazionale del notariato svolge l'attività nel rispetto dei pertinenti princìpi e delle regole tecniche previste nel medesimo CAD e predispone strumenti tecnici idonei a consentire, nei soli casi previsti dalla legge, l'accesso ai documenti conservati nella predetta struttura. Al riguardo, l'Ufficio del Garante nell'ambito di una proficua collaborazione con i competenti Uffici del Ministero della giustizia, aveva espresso forti perplessità sull'originaria formulazione di tale disposizione, evidenziando che il Consiglio nazionale del notariato dovrebbe avere solo un ruolo di gestore dell'infrastruttura informatica, predisponendo gli opportuni accorgimenti tecnici per rendere possibile l'accesso ai dati ai soli aventi diritto, senza tuttavia essere abilitato esso stesso al trattamento dei dati, se non nel caso di espressa previsione normativa. Le nuove disposizioni prevedono il parere del Garante per l'adozione di diversi decreti del Ministro della giustizia volti a dare attuazione alla riforma in oggetto, in particolare per quanto riguarda le regole tecniche per l'organizzazione della struttura predisposta dal Consiglio nazionale del notariato, per la trasmissione, conservazione e consultazione degli atti di cui agli artt. 62-*bis* e 62-*ter*, e per la formazione, conservazione e controllo dei repertori;

Mediazione

- il d.lgs. 4 marzo 2010, n. 28 che, in attuazione dell'art. 60 della l. 18 giugno 2009, n. 69, disciplina la mediazione finalizzata alla conciliazione delle controversie civili e commerciali. Il decreto attribuisce la funzione di svolgere il procedimento di mediazione a determinati "*organismi*", costituiti presso enti pubblici o privati che diano garanzie di serietà ed efficienza, iscritti in apposito registro istituito con decreto ministeriale. Chiunque presti servizio nell'organismo o comunque nell'ambito del

procedimento di mediazione è tenuto all'obbligo di riservatezza rispetto alle dichiarazioni rese e alle informazioni acquisite durante il procedimento medesimo (art. 9). Considerato che la mediazione può svolgersi secondo modalità telematiche (art. 3, comma 4), ciascun organismo con proprio regolamento deve prevedere "*le procedure telematiche eventualmente utilizzate dall'organismo, in modo da garantire la sicurezza delle comunicazioni e il rispetto della riservatezza dei dati*" (art. 16, comma 3). La materia oggetto del decreto legislativo è di particolare importanza sotto il profilo della protezione dei dati personali in quanto i predetti organismi devono effettuare un elevato numero di trattamenti di dati sensibili e giudiziari per l'espletamento delle attività ad essi riservate;

Servizi di pagamento

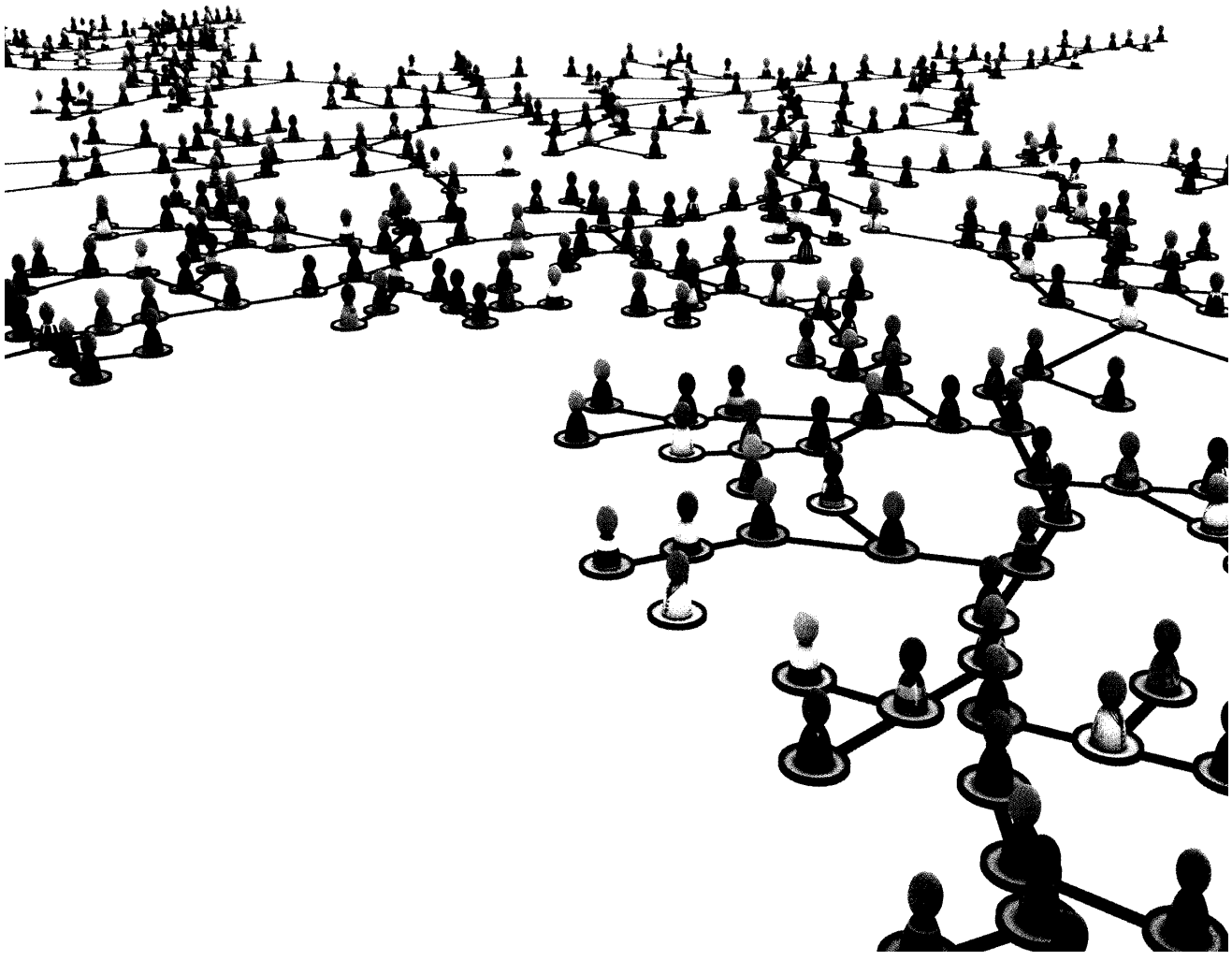
- il d.lgs. 27 gennaio 2010, n. 11, sull'"*Attuazione della Direttiva n. 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle Direttive nn. 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la Direttiva n. 97/5/CE*", che si applica ai servizi di pagamento prestati in euro o nella valuta ufficiale di uno Stato membro non appartenente all'area dell'euro o di uno Stato appartenente allo spazio economico europeo. I prestatori di servizi di pagamento e i gestori di sistemi di pagamento possono trattare dati personali in conformità al Codice, ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti;

Donazione di tessuti e cellule umani

- il d.lgs. 25 gennaio 2010, n. 16, recante attuazione delle Direttive nn. 2006/17/CE e 2006/86/CE, in materia di donazione, approvvigionamento e controllo di tessuti e cellule umani, il quale prevede, fra l'altro, "*nel rispetto delle norme per la tutela della riservatezza*", la tracciabilità dei tessuti e delle cellule donati, così garantendo peraltro un'adeguata identificazione del donatore (v. *Relazione* 2009, p. 57).

PAGINA BIANCA

L'attività svolta dal Garante



PAGINA BIANCA

II. L'attività svolta dal Garante

3. Il Garante e le pubbliche amministrazioni

3.1. I regolamenti sui trattamenti di dati sensibili e giudiziari

3.1.1. I regolamenti delle autorità indipendenti

Nel 2010 il Garante ha espresso parere favorevole su uno schema di delibera della CONSOB, volto a modificare il regolamento sul trattamento dei dati sensibili e giudiziari, in relazione all'istituzione, presso la stessa CONSOB, della Camera di conciliazione e arbitrato (*Parere* 8 aprile 2010 [doc. *web* n. 1718426]).

Anche la Banca d'Italia ha sottoposto all'Autorità uno schema di regolamento sul trattamento dei dati sensibili e giudiziari, volto a sostituire i precedenti regolamenti adottati dalla Banca d'Italia il 5 dicembre 2003 e dall'Ufficio italiano cambi il 25 maggio 2006, in ragione dell'avvenuto trasferimento alla Banca delle competenze del soppresso UIC, nonché dell'istituzione, presso il medesimo Istituto, dell'Unità di informazione finanziaria per l'Italia (UIF), con funzioni di prevenzione e contrasto dei fenomeni di riciclaggio di denaro e di finanziamento del terrorismo.

Il parere favorevole reso dall'Autorità è stato subordinato al rispetto del principio di indispensabilità nelle operazioni di comunicazione di dati sensibili riguardanti i pagamenti regolati dal sistema *TARGET2*, effettuate dalla Banca d'Italia su richiesta dell'UIF. In particolare l'Autorità ha evidenziato l'esigenza di specificare, nello schema di regolamento, che l'UIF può formulare richieste di dati soltanto "*al fine di integrare l'analisi delle operazioni sospette e lo studio dei flussi finanziari effettuati sulla base dei dati e delle informazioni di cui l'Ufficio viene a conoscenza ai sensi e per gli effetti della disciplina sulla prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo*" con riferimento "*a soggetti (persone fisiche e giuridiche) espressamente individuati*" (*Parere* 13 gennaio 2011 [doc. *web* n. 1787870]).

Il Garante ha infine espresso parere favorevole su uno schema di *regolamento* per il trattamento dei dati sensibili e giudiziari predisposto dall'Autorità per l'energia elettrica e il gas (*Parere* 3 febbraio 2011 [doc. *web* n. 1790422]).

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

Nel periodo di riferimento l'attività del Garante in questa materia si è svolta in due direzioni.

Da un lato la preparazione e poi, dopo la consultazione pubblica sullo schema approvato il 16 dicembre 2010, l'adozione delle "*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*" (*Provv.* 2 marzo 2011 [doc. *web* n. 1793203]); dall'altro, la trattazione di numerosi casi, dei quali alcuni *infra* esemplificati, che presentavano profili relativi all'accesso e alla trasparenza connessi, in vario modo, con aspetti inerenti la protezione dei dati personali.

Linee-guida sulla pubblicazione nel *web* da parte di pp.aa.

Le menzionate linee-guida hanno individuato i criteri e le cautele che i soggetti pubblici devono seguire nell'attuare le disposizioni, molte delle quali recenti, relative alla pubblicazione sul *web* di atti e documenti amministrativi. In sintesi, si evidenzia in primo luogo che la comunicazione e la diffusione di dati personali da parte di pp.aa. attraverso i propri siti istituzionali possono avvenire solo se previste da una norma (artt. 4, comma 1, lett. *l*) e *m*), 19, comma 3, 20 e 21, del Codice).

Per la pubblicazione di dati sensibili è necessaria un'espressa disposizione di legge, o del regolamento che l'amministrazione è tenuta ad adottare, che specifichi i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite, nel rispetto del generale divieto di diffusione dei dati idonei a rivelare lo stato di salute dei singoli interessati (artt. 22, comma 8, 65, comma 5, 68, comma 3, del Codice).

Le specifiche richieste degli interessati di pubblicare propri dati personali sul sito istituzionale dell'amministrazione potranno essere accolte se tale operazione risulti compatibile con lo svolgimento delle funzioni istituzionali e se i dati, oggetto di diffusione *online*, risultino pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11 del Codice).

Occorre pertanto individuare idonei accorgimenti volti ad assicurare forme corrette e proporzionate di conoscibilità di tali informazioni impedendo la loro indiscriminata reperibilità in Internet, garantendo il rispetto dei princìpi di qualità ed esattezza dei dati e delimitando la durata della loro disponibilità *online*.

Appare preferibile rendere reperibili i dati mediante motori di ricerca interni al sito, per assicurare accessi maggiormente coerenti con le finalità di volta in volta sottese alla pubblicazione, specialmente laddove si tratti, se non di dati sensibili, di dati comunque delicati, quali giudizi ovvero esiti concorsuali, assicurando, nel contempo, la conoscibilità sui siti istituzionali delle informazioni che si intende mettere a disposizione.

Se non stabiliti da specifiche disposizioni di settore, vanno inoltre individuati, a cura delle amministrazioni interessate, congrui periodi di tempo –non superiori a quanto ritenuto, caso per caso, necessario al raggiungimento degli scopi per i quali i dati stessi sono resi pubblici– entro i quali atti e documenti contenenti dati personali, devono rimanere disponibili *online* (in una forma che consenta l'identificazione dell'interessato).

Trascorsi tali periodi, i dati devono essere rimossi dal *web* ovvero inseriti in un'area di archivio consultabile solo a partire dal sito stesso e non raggiungibili utilizzando i motori di ricerca esterni, a tal fine adottando gli opportuni accorgimenti tecnici.

Devono essere adottate opportune cautele per evitare operazioni di duplicazione massiva dei *file* contenenti dati personali, rinvenibili sui siti istituzionali delle amministrazioni, mediante l'utilizzo di *software* o programmi automatici, al fine di ridurre il rischio di riproduzione e riutilizzo dei contenuti informativi in ambiti e contesti differenti, garantendo comunque l'accessibilità alle informazioni riprodotte *online* anche alle persone disabili, nel rispetto delle disposizioni della l. 9 gennaio 2004, n. 4.

I dati messi a disposizione *online* devono essere esatti, aggiornati e attendibili (art. 11, comma 1, lett. *c*), del Codice), anche alla luce dell'obbligo di garantirne la conformità alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione attraverso il sito (art. 54, comma 4, d.lgs. n. 82/2005, codice dell'amministrazione digitale), impiegando idonee misure per ridurre il rischio di alterazioni delle informazioni e dei documenti resi disponibili tramite Internet (ad es., indicando le fonti attendibili per il reperimento dei medesimi documenti, utilizzando certificati e firma digitale o inserendo, in ogni *file* oggetto di pubblicazione sui siti istituzionali, "*dati di contesto*" quali data di aggiornamento, periodo di validità, amministrazione).

Si riportano di seguito alcune delle fattispecie esemplificative evidenziate nelle linee-guida di cui trattasi.

Ove previsto l'obbligo di pubblicazione del modello di *curriculum* europeo, occorre selezionare i contenuti da riprodurre sui siti istituzionali in ragione unicamente delle finalità di trasparenza perseguite (art. 11, comma 8, lett. *e*), *f*), e *h*), d.lgs. n. 150/2009 e art. 21, comma 1, l. n. 69/2009) in base al principio di pertinenza e non eccedenza e in relazione alle funzioni pubbliche ricoperte dal personale interessato, al quale va garantita la possibilità di aggiornare periodicamente il proprio *curriculum*.

Non appare giustificato riprodurre sul *web* informazioni di dettaglio quali i cedolini dello stipendio, l'orario di lavoro effettivamente svolto dai dipendenti, i recapiti privati, ovvero informazioni attinenti allo stato di salute di persone identificate, quali le assenze verificatesi per ragioni di salute.

Nella sezione dei siti istituzionali dedicata a "*Trasparenza, valutazione e merito*", si ritiene che debbano essere privilegiati canali o modalità di ricerca interni ai medesimi siti limitando, attraverso idonei accorgimenti, l'indicizzazione da parte dei motori di ricerca esterni, nonché la creazione di copie *cache* presso gli stessi motori di ricerca.

Non si ravvisa la necessità di adottare alcuna specifica cautela per la pubblicazione di informazioni non riconducibili a persone identificate o identificabili (ad es., dati aggregati per Uffici riguardanti i livelli retributivi, i tassi di assenza e di maggiore presenza del personale; l'ammontare complessivo dei premi collegati alla *performance* stanziati e di quelli effettivamente distribuiti; obiettivi assegnati agli Uffici ed i relativi indicatori; dati relativi al grado di differenziazione nell'utilizzo della premialità, informazioni concernenti la dimensione della qualità dei servizi erogati, notizie circa la gestione dei pagamenti e le buone prassi).

Restano salve le specifiche previsioni sulla conoscibilità delle situazioni patrimoniali di chi riveste cariche pubbliche.

In considerazione dell'ampio regime di conoscibilità previsto per i dati raccolti dal Ministero dell'interno nell'anagrafe degli amministratori locali e regionali (art. 76 del d.lgs. n. 267/2000), di cui chiunque ha il diritto di prendere visione ed estrarre copia,

anche su supporto informatico, gli atti statutari, legislativi o regolamentari delle amministrazioni regionali e degli enti locali interessati possono autorizzarne la messa a disposizione per via telematica attraverso i propri siti istituzionali.

Con riferimento ai ruoli dei dirigenti che ciascuna amministrazione dello Stato deve pubblicare sul proprio sito *web*, vanno rese pubbliche le sole informazioni individuate nel dettaglio dalla disciplina di settore (cognome, nome, luogo e data di nascita; data di inquadramento nella fascia di appartenenza o in quella inferiore; data di primo inquadramento nell'amministrazione; incarichi conferiti ai sensi dell'art. 19, commi 3 e 4, del d.lgs. 30 marzo 2001, n. 165 con l'indicazione della decorrenza e del termine di scadenza) (artt. 1, comma 7, e 2, commi 1 e 3, d.P.R. 23 aprile 2004, n. 108).

Diversamente, la banca dati informatica dei ruoli delle amministrazioni dello Stato, istituita presso il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, che contiene ulteriori informazioni professionali (art. 2, comma 4, d.P.R. n. 108/2004 e artt. 23, comma 2, e 28, comma 7-*bis*, d.lgs. 30 marzo 2001, n. 165) va resa accessibile esclusivamente alle pp.aa. interessate al conferimento di incarichi dirigenziali nonché a coloro che ne abbiano interesse per la tutela di situazioni giuridicamente rilevanti.

Nel mettere a disposizione in rete i ruoli di anzianità del personale ed i bollettini ufficiali che le amministrazioni devono pubblicare mensilmente, occorre evitare l'inserimento di notizie non pertinenti, in particolare quelle idonee a rivelare dati sensibili (ad es., mutilato o invalido civile; aspettativa per motivi di salute o distacco per motivi sindacali), anche adottando idonei accorgimenti quali l'utilizzo di *omissis*, diciture generiche o codici numerici (art. 24, commi 1 e 3, d.P.R. 3 maggio 1957, n. 686).

Nell'albo dei beneficiari di provvidenze di natura economica (d.P.R. 7 aprile 2000, n. 118) 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, ove questa non sia idonea a rivelare lo stato di salute degli interessati (ad es., l. 12 marzo 1999, n. 68, recante *"Norme per il diritto al lavoro dei disabili"*).

In ogni caso, non devono 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) con riferimento all'indicazione dei titoli dell'erogazione dei benefici (ad es., attribuzione di borse di studio a "*soggetto portatore di handicap*") e dei criteri di attribuzione (ad es., punteggi attribuiti con l'indicazione degli "*indici di autosufficienza nelle attività della vita quotidiana*", *cd.* "*scala Adl*" o "*di Katz*").

Nella pubblicazione di graduatorie, esiti e giudizi concorsuali può essere opportuno, in particolare, attribuire ai concorrenti credenziali di autenticazione (ad es., *username* o *password*) per consentire l'accesso ad aree del sito istituzionale in cui eventuali ulteriori informazioni siano rese disponibili ai soli aventi diritto sulla base della normativa in materia di accesso ai documenti amministrativi (quali elaborati, verbali, titoli di precedenza o preferenza).

Devono ritenersi pertinenti ai fini della pubblicazione *online* gli elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, gli elenchi di ammessi a prove scritte o orali, i punteggi riferiti a singoli argomenti di esame, i punteggi totali ottenuti non, invece, dati eccedenti quali i titoli di studio, il codice fiscale, numero di figli disabili, i risultati di *test* psicoattitudinali.

Analoghe cautele devono essere adottate in relazione alle pubblicazioni effettuate nel quadro delle ordinarie attività di gestione di rapporti di lavoro (ad es., graduatorie di mobilità professionale).

Ove, in base a specifiche disposizioni, siano determinabili a priori i soggetti legittimati a conoscere informazioni detenute dalle pp.aa. (ad es., destinatari del *provvedimento*, terzi interessati e contro interessati, ecc.), non è in linea di principio proporzionato consentire l'accesso *online* libero e incondizionato, senza applicare criteri selettivi, alla consultazione di atti e documenti contenenti informazioni personali, specie se aventi natura sensibile.

Per gli elenchi del collocamento obbligatorio dei disabili (che contengono i nominativi degli interessati associati allo stato di disabilità o all'appartenenza alle altre categorie di aventi diritto al collocamento), le amministrazioni devono adottare idonei accorgimenti volti a impedire che vengano diffusi dati sulla salute (artt. 22, comma 8 e 68, comma 3, del Codice), rendendo conoscibili le informazioni ivi riportate unicamente ai soggetti

richiedenti, per le sole finalità previste dalla normativa di riferimento o a coloro che vi abbiano interesse per la tutela di situazioni giuridicamente rilevanti (ad es., attribuendo a tali soggetti idonee credenziali di accesso, quali *username* o *password*, numero di protocollo o altri estremi correlati alla richiesta di iscrizione nelle liste, ovvero predisponendo, nei siti istituzionali, aree ad accesso parimenti selezionato).

Casistica in materia di accesso e trasparenza amministrativa

Per quanto attiene, invece, alla casistica delle questioni oggetto di intervento dell'Autorità, ad una segnalante che aveva lamentato il rifiuto opposto da una p.a. ad una sua richiesta di accesso ad atti amministrativi, l'Ufficio ha evidenziato che spetta all'amministrazione destinataria e non all'Autorità verificare, caso per caso, la fondatezza della richiesta di accesso (*Nota* 16 luglio 2010).

Analoghe considerazioni sono state espresse al Ministero degli affari esteri che aveva chiesto chiarimenti in ordine all'effettiva sussistenza di un obbligo giuridico di rendere ostensibili taluni atti formati o comunque rientranti nella disponibilità del predetto Ministero e degli Uffici all'estero, alla luce del d.m. 7 settembre 1994, n. 604, con cui sono state individuate le categorie di documenti esclusi dal diritto di accesso secondo quanto previsto all'art. 24, comma 2, della l. 7 agosto 1990, n. 241 (*Nota* 9 giugno 2010).

Sostanziale analoga risposta è altresì stata data ad una segnalante che lamentava di non essere stata interpellata, pur essendo controinteressata, in ordine ad una richiesta di accesso a taluni documenti amministrativi (*Nota* 9 giugno 2010).

Con riferimento ad una segnalazione relativa alla produzione in giudizio di documenti contenenti dati personali dell'interessata, l'Ufficio ha precisato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali restano disciplinate dalle pertinenti disposizioni processuali (art. 160, comma 6, del Codice) (*Nota* 11 gennaio 2011).

Anche durante l'anno di riferimento, sono emerse talune problematiche riguardanti il diritto di accesso dei consiglieri comunali e provinciali agli atti dell'ente di appartenenza.

Ad una richiesta della Commissione per l'accesso ai documenti amministrativi sull'ostensibilità ad un consigliere provinciale di informazioni riguardanti le rilevazioni della presenza del personale della polizia provinciale (turni di servizio, timbrature delle presenze

effettuate con *badge* e presenze attestate mediante fogli), l'Ufficio ha ricordato che il diritto dei consiglieri comunali e provinciali di ottenere dagli enti "*tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato*" riguarda tutto ciò che può essere effettivamente funzionale allo svolgimento dei compiti del singolo consigliere, per valutare con piena cognizione di causa l'operato dell'amministrazione, oltre che per promuovere le iniziative che spettano ai singoli rappresentati (art. 43, comma 2, d.lgs. 18 agosto 2000, n. 267) (*Nota* 6 aprile 2010).

L'Ufficio non ha ravvisato gli estremi per promuovere l'adozione di specifici provvedimenti (artt. 11, comma 1, lett. *b*), e 13, comma 4, del regolamento del Garante n. 1/2007) in relazione alla segnalazione di un comune sulla presunta violazione della disciplina in materia di protezione dei dati personali da parte di un consigliere comunale, che aveva trasmesso a talune testate giornalistiche una serie di documenti amministrativi ottenuti in base all'art. 43, comma 2, d.lgs. n. 267/2000; non è infatti risultata provata la violazione di un segreto "*specificamente determinato dalla legge*", né di divieti di divulgazione dei dati personali previsti dal Codice (ad es., art. 22, comma 8, che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (*Nota* 17 giugno 2010).

Ad un comune che aveva chiesto se, per evadere la richiesta di un consigliere comunale di ottenere copia delle dichiarazioni dei redditi del sindaco e di tutti gli assessori, occorresse reperire tali informazioni tramite l'accesso al sistema Siatel, è stato rappresentato che le norme riconoscono ai consiglieri comunali e provinciali il diritto di ottenere dagli Uffici, rispettivamente del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni "*in loro possesso*" utili all'espletamento del proprio mandato (art. 43, comma 2, d.lgs. n. 267/2000) (*Nota* 26 gennaio 2011).

Sono stati molto numerosi anche i casi di diffusione di dati personali effettuata da soggetti pubblici per dare pubblicità alla propria attività istituzionale, specie tramite l'impiego di tecniche informatiche e telematiche.

Un comune che aveva chiesto chiarimenti in ordine alla possibilità di pubblicare i dati catastali attraverso il proprio sito *web* (e, separatamente, nel sistema informativo territoriale) rendendoli disponibili alla libera consultazione, è stato invitato a verificare se

l'iniziativa fosse conforme alle specifiche disposizioni di settore vigenti, nonché alle recenti norme in materia di anagrafe immobiliare integrata di cui all'art. 19 del d.l. 31 maggio 2010, n. 78 recante "*Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica*" (cfr. "*Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali*", *Provv.* 19 aprile 2007 [doc. *web* n. 1407101]; *Relazione* 2007, p. 40) (*Nota* 9 giugno 2010).

In un caso diverso, era stata lamentata la diffusione, tramite il sito istituzionale di un comune, di due verbali di deliberazioni della giunta, recanti le generalità dei beneficiari di iniziative volte all'inserimento socio-lavorativo di portatori di *handicap*. Una delle delibere era risultata altresì visualizzabile anche tramite i più diffusi motori di ricerca esterni al sito istituzionale.

L'Ufficio ha invitato il comune a rispettare il divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati attivandosi, altresì, al fine di impedire l'indicizzazione dei predetti documenti da parte dei principali motori di ricerca esterni (in particolare, *Google* e *Yahoo*) richiedendo anche la rimozione, entro un congruo periodo di tempo, dei suddetti contenuti memorizzati nella *cache*. Avendo ricevuto idonee assicurazioni in merito, non sono stati adottati specifici provvedimenti (*Nota* 18 agosto 2010).

L'Autorità è stata interpellata dal Ministero per la pubblica amministrazione e l'innovazione in ordine alla possibilità di pubblicare, da parte delle amministrazioni interessate, informazioni sulla situazione patrimoniale dei titolari di cariche elettive e di cariche direttive di alcuni enti pubblici, ai sensi della l. 5 luglio 1982, n. 441. In proposito, è stato rappresentato, in particolare, che occorre rispettare i limiti previsti da tale legge in base alla quale, in particolare, per le regioni è prevista la pubblicazione dei dati in parola sul bollettino regionale, liberamente disponibile e acquistabile da chiunque (art. 11). Le amministrazioni diverse dalle regioni, invece, possono mettere i dati a disposizione esclusivamente dei "*cittadini iscritti nelle liste elettorali per le elezioni della Camera dei deputati*", e quindi, se i dati sono pubblicati sui siti istituzionali, esse devono adottare gli accorgimenti tecnici per limitare alle menzionate categorie di soggetti l'accesso a tali informazioni, previa informativa agli interessati circa tale modalità di diffusione (*Nota* 27 luglio 2010).

3.3. LA DOCUMENTAZIONE ANAGRAFICA E LA MATERIA ELETTORALE

Anagrafi della popolazione

Il trattamento dei dati contenuti nelle anagrafi della popolazione residente presso i comuni ha continuato a porre numerose problematiche applicative, sulle quali sono state spesso chieste al Garante delucidazioni.

Al riguardo, in diverse occasioni è stato rappresentato che il comune deve rilasciare elenchi degli iscritti nell'anagrafe della popolazione residente solamente a pp.aa. "*che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità*" (art. 34, commi 1 e 2, d.P.R. 30 maggio 1989, n. 223).

Alle forze dell'ordine è consentito consultare direttamente gli atti anagrafici, previa comunicazione all'ufficiale di anagrafe delle generalità del personale abilitato alla consultazione, il quale opererà secondo modalità tecniche adottate d'intesa tra gli uffici anagrafici comunali e gli organi interessati (art. 37, commi 1 e 4, d.P.R. 30 maggio 1989, n. 223) (*Nota* 3 dicembre 2010).

Il comune, al pari di qualunque soggetto pubblico, può avvalersi di un soggetto privato –designandolo responsabile del trattamento– per affidargli determinate attività, che restano nella sua sfera di titolarità (*Nota* 21 dicembre 2010, relativa alla trasmissione di dati anagrafici ad un consorzio).

Per quanto riguarda la gestione in *outsourcing* dell'anagrafe della popolazione residente, sono state richiamate le specifiche garanzie già individuate nel *provvedimento* 6 ottobre 2005 [doc. *web* n. 1179484] (*Nota* 18 agosto 2010). In tali casi e negli altri in cui una puntuale disposizione normativa preveda la comunicazione ad altri soggetti pubblici, il comune deve solo applicare le norme, senza necessità di rivolgersi al Garante (v. anche art. 19, comma 2, del Codice). I dati raccolti devono essere pertinenti e non eccedenti rispetto agli scopi perseguiti (art. 11, comma 1, lett. *d*), del Codice).

In questo quadro generale, si cita il quesito di un comune circa la legittimità della trasmissione dei dati anagrafici riguardanti gli intestatari dei fogli di famiglia ed i coniugi, ad una società a totale capitale pubblico, che effettua il servizio di verifica degli impianti termici per conto di una provincia, al fine di informare gli utenti in ordine a taluni aspetti connessi all'utilizzo dei predetti impianti.

Al riguardo, in conformità al quadro normativo di settore (art. 17, comma 1, del d.P.R. 21 dicembre 1999, n. 551), è stato fatto presente che il comune può comunicare i suddetti dati alla provincia, la quale può legittimamente avvalersi di un soggetto esterno nell'ambito di un rapporto fra titolare e responsabile del trattamento (art. 29 del Codice), al fine di perseguire la finalità istituzionale rappresentata (*Nota* 6 luglio 2010).

In un altro caso, in relazione alla richiesta dell'attivazione di una convenzione, tra una società a totale partecipazione pubblica preposta alla gestione della tariffa rifiuti, ed una società fornitrice dei *software* gestionali di un comune, al fine di allineare dati personali detenuti dal gestore con quelli dell'anagrafe della popolazione residente riprodotti su una *cd.* "*server farm*" della predetta società, sono state richiamate le norme in materia di trasmissibilità dei dati anagrafici ed il quadro di garanzie sull'affidamento in *outsourcing* della gestione dell'anagrafe della popolazione residente (*Nota* 18 agosto 2010, cit. *supra*).

Materia elettorale

Sono state poche, invece, le questioni sottoposte all'Autorità in materia elettorale, ed in proposito, si cita, in particolare una segnalazione relativa alla ricezione di materiale di propaganda elettorale inviate da un candidato ad un consiglio regionale, che in passato aveva ricoperto la carica di assessore regionale alla protezione civile.

L'Ufficio ha invitato la segnalante ad esercitare il diritto di accesso ai propri dati personali ai sensi dell'art. 7 del Codice, per verificarne l'origine e le modalità del trattamento od opporsi al loro utilizzo, ad esempio all'ulteriore ricezione di materiale o chiamate (*Nota* 17 giugno 2010).

In questi casi, occorre infatti distinguere tra dati utilizzabili senza il consenso dell'interessato, quali le informazioni estratte da registri, elenchi, atti o documenti detenuti da un soggetto pubblico e liberamente accessibili per espressa disposizione normativa, e dati conosciuti in relazione ad un'attività o ad un servizio svolti (ad es., in una struttura *no profit*), utilizzabili solo con il consenso (*Provv.* 11 febbraio 2010 [doc. *web* n. 1694531], in *G.U.* 22 febbraio 2010, n. 43, che richiama il *provvedimento* generale 7 settembre 2005 [doc. *web* n. 1165613]).

3.4. L'ISTRUZIONE

3.4.1. La scuola

Nel corso dell'anno di riferimento l'Autorità è intervenuta più volte in materia di trattamento di dati personali in ambito scolastico.

In particolare, era stato segnalato all'Autorità che un comune, per prevenire eventuali abusi, forniva buoni pasto di colori differenti in relazione alla fascia di reddito di appartenenza delle famiglie degli studenti beneficiari, rendendo così conoscibile a chiunque accedesse alle mense scolastiche le condizioni di reddito delle famiglie. Facendo seguito alla richiesta di informazioni ed alle indicazioni del Garante, il comune ha garantito che sarebbero stati stampati buoni pasto dello stesso colore per tutti i beneficiari, indipendentemente dalla fascia di reddito di appartenenza, che potrà così evincersi solo dalle lettere "A" e "B" apposte su ogni singolo buono (*Nota* 17 dicembre 2010).

I genitori di uno studente avevano segnalato l'avvenuta comunicazione da parte di una scuola ad un esercizio commerciale degli elenchi comprensivi di generalità e classe degli studenti, per consentire di individuare le divise scolastiche da fornire.

In un altro caso, il Garante ha vietato l'ulteriore comunicazione dei dati degli allievi a qualsiasi soggetto privato, in assenza di una specifica norma di legge o di regolamento (art. 19, comma 3, del Codice; artt. 143, comma 1, lett. *c*) e 154, comma 1, lett. *d*), del Codice) (*Provv.* 13 maggio 2010 [doc. *web* n. 1738356]).

L'Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione (INVALSI) aveva effettuato una comunicazione al Garante per poter trasmettere all'Ufficio scolastico regionale della Lombardia che ne aveva fatto richiesta, in mancanza di apposita normativa, "*i dati relativi agli esiti della prova nazionale svolta nell'ambito dell'esame di stato conclusivo del primo ciclo di istruzione, disaggregati a livello di scuola e di classe*" (artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice).

L'Ufficio ha al riguardo fatto presente che l'INVALSI, quale ente di ricerca di diritto pubblico (art. 2, comma 2, d.lgs. 19 novembre 2004, n. 286) può comunicare dati personali a soggetti diversi da un'università o istituto o ente di ricerca o ricercatore, che ne facciano richiesta per il perseguimento di scopi non di natura statistica, solo in forma

aggregata o secondo modalità che non rendano identificabili gli interessati neppure tramite identificativi indiretti (art. 8, comma 1, codice di deontologia e di buona condotta, Allegato A.4. al Codice, cit.) (*Nota* 4 ottobre 2010).

Ad una regione, che aveva chiesto chiarimenti per costituire la propria anagrafe regionale degli studenti, il Garante, dopo aver precisato che il sistema nazionale delle anagrafi è composto dall'anagrafe nazionale degli studenti, dalle anagrafi regionali degli studenti e dalle anagrafi comunali della popolazione, in particolare ha evidenziato che il Ministero dell'istruzione dell'università e della ricerca ha adottato, sentito il Garante (*Parere* 16 giugno 2010 [doc. *web* n. 1734404]), un decreto con il quale ha istituito l'anagrafe nazionale degli studenti, individuando i tipi di dati che devono confluirvi ed i soggetti legittimati ad accedervi (d.m. 5 agosto 2010) (*Nota* 24 settembre 2010).

3.4.2. L'università

L'Autorità ha fornito alcuni chiarimenti anche alle università, in ordine alle corrette modalità di trattamento dei dati personali riferiti agli studenti.

In particolare, era pervenuta all'Ufficio una segnalazione anonima con la quale veniva evidenziato che un'università, nel pubblicare sul proprio sito Internet l'elenco dei candidati iscritti ad alcuni esami di abilitazione, diffondeva anche informazioni idonee a rivelare lo stato di salute degli interessati, desumibili dalla voce "ausilio *hand*" indicata nei suddetti elenchi. Facendo seguito alla richiesta di informazioni ed alle indicazioni dell'Ufficio relative, in particolare, al divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (art. 22, comma 8, del Codice), l'ateneo ha eliminato tale voce dalle griglie delle graduatorie, rimosso dal proprio sito Internet il *link* per l'accesso ai *file* contenenti i suddetti elenchi, richiedendo altresì al motore di ricerca *Google* l'immediata eliminazione dei menzionati indirizzi Internet (*Note* 18 ottobre e 25 novembre 2010).

3.5. ATTIVITÀ FISCALE, TRIBUTARIA E DOGANALE

Il Garante, completata l'istruttoria sulla nuova classe di servizi di cooperazione applicativa, *cd.* "*web service*", realizzata dall'Agenzia delle entrate per l'accesso all'anagrafe tributaria

da parte di INPS, INPDAP, ENPALS, AVCP, camere di commercio e AGEA, ha impartito ulteriori prescrizioni volte a rafforzare la protezione dei dati personali (*Provv.* 26 marzo 2010 [doc. *web* n. 1713453]), in aggiunta a quelle già individuate nel *provvedimento* 18 settembre 2008 [doc. *web* n. 1549548].

Per la difficoltà del passaggio alla nuova classe di *web* service e l'esigenza di continuità delle funzioni istituzionali perseguite dai suddetti enti, sono stati prorogati i termini previsti nel cit. *provvedimento* 18 settembre 2008, in particolare al:

- 31 ottobre 2010, per il passaggio alla nuova classe di *web* service da parte di INPS, INPDAP, AVCP e ENPALS, nonché al collegamento denominato "3270 enti esterni" con INPS, camere di commercio e AGEA (*Provv.* 26 marzo 2010 [doc. *web* n. 1713453]);
- 31 dicembre 2010, per l'adempimento della prescrizione di cui alla lett. *d*), II), secondo punto, del cit. *provvedimento* 18 settembre 2008 limitatamente ai suddetti enti esterni, ai fini del completamento dell'*iter* di trasferimento dei *web service* all'interno del sistema pubblico di connettività, istituito dal codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82) (*Provv.* 2 dicembre 2010 [doc. *web* n. 1776140]);
- 15 febbraio 2011, per l'adempimento della prescrizione di cui alla lett. *a*), *I*), secondo punto, del cit. *provvedimento* 18 settembre 2008 con riferimento al completamento della procedura di stipula delle convenzioni (*Provv.* 21 ottobre 2010 [doc. *web* n. 1767204]).

Nel *provvedimento* 26 marzo 2010 il Garante ha prescritto che i *web service* possano essere utilizzati esclusivamente da utenti il cui codice sia preventivamente comunicato all'Agenzia delle entrate dall'ente di appartenenza, per i soli dati necessari a ciascuna specifica interrogazione, la quale deve individuare puntualmente il soggetto cui si riferiscono le informazioni richieste. Inoltre, l'Agenzia deve attivare degli *alert* per individuare comportamenti anomali o a rischio e trasporre tali condizioni d'uso in appositi "accordi di servizio".

Più in dettaglio INPS, INPDAP, ENPALS, AVCP, camere di commercio e AGEA devono utilizzare questi servizi solo per finalità istituzionali per le quali è consentita la comunicazione, da parte dell'Agenzia delle entrate, delle informazioni contenute nell'anagrafe

tributaria. Con tali applicativi, inoltre, l'utente potrà acquisire solo informazioni pertinenti e non eccedenti le finalità perseguite; al tal fine, ciascun ente dovrà concordare con l'Agenzia le differenti tipologie di *web service* necessari.

Inoltre, ciascun ente deve designare incaricato del trattamento ed abilitare espressamente gli utenti all'utilizzo dei *web service*, comunicando preventivamente il relativo codice all'Agenzia. I *web service* non possono, quindi, essere utilizzati da soggetti esterni ai suddetti enti.

Il Garante ha successivamente stabilito che l'Agenzia delle entrate possa consentire l'utilizzo dei *web service* da parte di INPS, INPDAP, ENPALS, AVCP, camere di commercio e AGEA anche in assenza della suddetta previa comunicazione. Ciò in considerazione delle complessità dell'adempimento e del fatto che l'attuale cornice di sicurezza consente già la tracciabilità degli accessi. Gli enti che intendano avvalersi di tale facoltà devono predisporre soluzioni che consentano all'Agenzia di ricevere tempestivamente informazioni relative a singole utenze, per il monitoraggio di eventuali utilizzi impropri dei collegamenti (*Provv.* 2 dicembre 2010 [doc. *web* n. 1776140]).

Il Garante ha altresì deciso, in particolare, che l'INPS può avvalersi dei *web service* dell'Agenzia predetta anche nell'ambito degli applicativi utilizzati dai cittadini e dai loro intermediari (quali, ad es., CAF e commercialisti) solo per la verifica delle informazioni da questi comunicate, anche in riferimento ai dati identificativi di altri soggetti, avendo l'Agenzia stessa garantito la possibilità di ricondurre le operazioni effettuate alla persona fisica che le ha originate. Ciò in considerazione delle garanzie offerte dall'Agenzia e della particolare procedura individuata al fine di consentire l'adeguata tracciabilità di tali accessi all'anagrafe tributaria (*Provv.* 9 dicembre 2010 [doc. *web* n. 1780265]).

Il Garante ha espresso infine parere favorevole sullo schema di *provvedimento* del direttore dell'Agenzia delle entrate concernente le "*modalità tecniche relative alla trasmissione da parte dei comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero, in attuazione dell'art. 83, comma 16, d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla l. n. 133 del 6 agosto 2008*" (*Parere* 2 dicembre 2010 [doc. *web* n. 1779678]).

3.6. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

In molteplici casi, in situazioni spesso assai diverse, alcune delle quali sono di seguito esemplificate, l'Ufficio è intervenuto su impulso dei cittadini chiedendo chiarimenti o invitando i titolari del trattamento al rispetto delle disposizioni vigenti.

In dettaglio, su richiesta di una segnalante, che aveva lamentato la visibilità delle generalità della persona fisica interessata sui contrassegni rilasciati per la circolazione e la sosta di veicoli a servizio di persone invalide, l'Ufficio ha ottenuto dal comune competente idonee assicurazioni sul rispetto delle regole, in base alle quali le generalità della persona interessata devono essere riportate "*con modalità che non consentono … la loro diretta visibilità se non in caso di richiesta di esibizione o necessità di accertamento*" (art. 74, comma 2, del Codice).

Sulla base delle assicurazioni ricevute, l'Ufficio non ha intrapreso iniziative per l'adozione di specifici provvedimenti in relazione a quanto segnalato (artt. 11, comma 1, lett. *d*), e 13, comma 4, del regolamento del Garante n. 1/2007) (*Nota* 9 giugno 2010).

Ad una cittadina che aveva chiesto se il personale incaricato potesse ispezionare il contenuto dei sacchetti per identificare i trasgressori delle prescrizioni relative alla raccolta differenziata dei rifiuti, è stato risposto affermativamente, richiamando le specifiche garanzie al riguardo indicate al punto 4, lett. *d*), del *provvedimento* 14 luglio 2005 [doc. *web* n. 1149822] (*Nota* 6 luglio 2010).

Sempre in materia, un comune, interpellato dall'Ufficio, in relazione ad una segnalazione nella quale era stata lamentato l'obbligo di inserire i rifiuti cartacei aperti, negli appositi cassonetti per la raccolta differenziata, ha rappresentato che, in alternativa, vi era anche la possibilità di avvalersi di altre idonee modalità, tra cui il conferimento dei propri rifiuti cartacei presso lo stabilimento consortile, area ecologica liberamente accessibile a tutti. Alla segnalante è stata pertanto fatta presente l'insussistenza di violazioni (*Nota* 27 dicembre 2010).

Ad un altro comune, che aveva chiesto chiarimenti in ordine alla modalità di trattamento dei dati personali effettuati da parte di più soggetti esterni all'amministrazione, per l'attività di sviluppo e stampa della immagini di violazioni al codice della strada rilevate tramite fotocamera, è stato fatto presente che possono essere designati "responsabili" o

"incaricati" del trattamento più soggetti esterni, in conformità a quanto previsto dagli artt. 29 e 30 del Codice (*Nota* 6 luglio 2010).

Alla luce di notizie di stampa, l'Ufficio ha chiesto ad un comune di chiarire le cautele adottate per la notificazione di verbali relativi alle contravvenzioni al codice della strada in tema di atti contrari alla pubblica decenza in luogo pubblico. Avendo ricevuto idonee assicurazioni dal comune in ordine alla ritualità sia dell'ordinanza, sia della notificazione, mediante piego raccomandato privo di indicazioni relative al contenuto dell'atto e senza allegazione di prove documentali, l'Ufficio non ha ravvisato i presupposti per adottare un *provvedimento* del Collegio.

Un comune, formalmente interessato dall'Ufficio in relazione ad una segnalazione che aveva lamentato l'invio di un modello recante, su un lato visibile a tutti, l'indicazione relativa a provvidenze economiche in favore di minorati civili, ha dichiarato di aver erroneamente adoperato uno stampato non più in uso fornendo idonee assicurazioni per i trattamenti successivi. A fronte di ciò, l'Ufficio non ha intrapreso iniziative per l'adozione di specifici provvedimenti (artt. 11, comma 1, lett. *d*), e 13, comma 4, del regolamento del Garante n. 1/2007) (*Nota* 1 aprile 2010).

Da un'altra segnalazione era emerso che il testo di un messaggio di posta elettronica inviato ad un assessore era stato acquisito dal sindaco e letto in occasione di una seduta del consiglio comunale. Al riguardo, poiché il comune, cui l'Ufficio aveva richiesto chiarimenti, ha informato di aver adottato una delibera di giunta sul rispetto delle regole e degli accorgimenti indicati nelle "*Linee-guida per posta elettronica e Internet*" (*Provv.* 1 marzo 2007 [doc. *web* n. 1387522]), l'Ufficio non ha ravvisato i presupposti per l'adozione di provvedimenti (v. artt. 11, comma 1, lett. *d*), e 13, comma 4, del regolamento del Garante n. 1/2007) (*Nota* 21 gennaio 2011).

La Regione autonoma Friuli Venezia Giulia aveva sottoposto al Garante uno schema di disposizione per modificare la normativa sui candidati alle consultazioni elettorali regionali (art. 17 della l.r. 28/2007) per consentire, in base ad una specifica manifestazione di volontà scritta del candidato, "*l'accesso ai dati contenuti nella sua autodichiarazione a chiunque ne faccia richiesta*", in modo che gli "*elettori, nello scegliere il candidato*

da votare", possano "*tenere in considerazione anche le eventuali condanne penali subite dallo stesso*".

Il Garante con *provvedimento* 3 febbraio 2011 [doc. *web* n. 1790414] ha ritenuto che il trattamento dei dati giudiziari fosse indispensabile per una finalità di rilevante interesse pubblico (artt. 20 e 21 del Codice).

Pertanto, l'Autorità non ha formulato osservazioni sullo schema di disposizione legislativa, a condizione che la Regione, da un lato, individui un congruo periodo di tempo, commisurato allo svolgimento delle elezioni regionali ed alla proclamazione degli eletti, entro il quale mantenere accessibili, a chiunque ne faccia richiesta, i suddetti dati personali; dall'altro, che nell'informativa fornita agli interessati evidenzi che i dati giudiziari, sulla base della specifica manifestazione di volontà degli interessati stessi, potranno essere comunicati a chiunque ne faccia richiesta (art. 13 del Codice).

3.7. COMUNICAZIONI DI DATI PERSONALI TRA SOGGETTI PUBBLICI

Nell'anno di riferimento numerosi soggetti pubblici hanno effettuato una comunicazione al Garante per trasmettere ad un altro soggetto pubblico, in assenza di una norma che lo preveda, dati personali –diversi da quelli sensibili e giudiziari– necessari per lo svolgimento di funzioni istituzionali (artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice).

Si segnalano in particolare, la comunicazione da parte del Ministero dello sviluppo economico ai competenti uffici delle camere di commercio industria e artigianato, che ne avevano fatto richiesta, dei dati dei soggetti che partecipano ai concorsi a premio, raccolti nel *database* del servizio PREMA presso la Direzione del ministero, (art. 12, d.P.R. 26 ottobre 2001, n. 430). Tale comunicazione è stata ritenuta legittima in ragione degli specifici compiti di verifica attribuiti, dalla normativa di settore, al responsabile della tutela del consumatore e della fede pubblica presso le camere di commercio (*Provv.* 3 giugno 2010 [doc. *web* n. 1734810]).

La Consigliera di parità della Regione Lombardia aveva chiesto al Ministero del lavoro e delle politiche sociali-Direzione provinciale del lavoro di Milano alcune informazioni (generalità, numero telefonico, anno di inizio lavoro e anno di decorrenza delle dimissioni,

azienda) relative alle lavoratrici madri che hanno presentato le dimissioni dal 2005 al 2008 ai fini della realizzazione del progetto "*Maternità e occupazione*", volto, in particolare ad offrire servizi alle donne che si sono dimesse. Tenuto conto di quanto previsto dalla normativa di settore ovvero delle circostanze che le consigliere ed i consiglieri di parità possono rilevare le situazioni di squilibrio di genere, per svolgere funzioni promozionali e di garanzia contro le discriminazioni sul lavoro (art. 15, comma 4, d.lgs. n. 11 aprile 2006, n. 198), il Garante ha stabilito che tale comunicazione possa avere luogo, prescrivendo che la Consigliera di parità debba conservare i dati non oltre il termine del progetto e che l'eventuale diffusione degli stessi avvenga secondo modalità che non consentano di risalire agli interessati, neppure tramite dati identificativi indiretti (*Provv.* 1 luglio 2010 [doc. *web* n. 1737773]).

Il Ministero dell'interno-Dipartimento della pubblica sicurezza-Direzione centrale dell'immigrazione e della polizia delle frontiere, aveva comunicato al Garante la richiesta delle aziende sanitarie locali di ottenere dalle questure gli elenchi degli stranieri presenti in provincia, per verificarne le posizioni e semplificare la prassi, che prevede l'esibizione del titolo di soggiorno all'atto del primo rilascio o del rinnovo dell'iscrizione al servizio sanitario nazionale. Al riguardo considerato che la normativa di settore già disciplina le modalità di iscrizione al SSN da parte degli stranieri in possesso di permesso di soggiorno, nonché di comunicazione alle aziende unità sanitarie locali delle ipotesi di mancato rinnovo, revoca o annullamento del permesso di soggiorno o di espulsione dello straniero (art. 34, comma 1, d.lgs. 25 luglio 1998, n. 286; artt. 42, commi 1 e 4, d.P.R. 31 agosto 1999, n. 394), il Garante ha ritenuto che non possano essere attivati flussi di dati diversi, anche attraverso le modalità previste dagli artt. 19, comma 2, e 39 comma 1, lett. *a*), del Codice (*Nota* 28 luglio 2010).

L'Ufficio ha poi fornito chiarimenti a due aziende sanitarie venete, alle quali l'Ente nazionale di previdenza ed assistenza medici aveva chiesto i dati relativi ai fatturati, suddivisi per branca specialistica, dei soggetti accreditati con il SSN, per verificare l'adempimento degli obblighi di cui all'art. 1, comma 39, della l. 23 agosto 2004, n. 243, relativi al versamento del contributo da parte delle società operanti in regime di accreditamento con il SSN.

Al riguardo, è stato rappresentato che, in considerazione della natura di diritto privato dell'ENPAM (art. 1, comma 2, d.lgs. 30 giugno 1994, n. 509), spetta alle citate amministrazioni verificare che la comunicazione rientri tra quelle previste dall'art. 19, comma 3, del Codice, che consente la comunicazione di dati personali da parte di un soggetto pubblico a privati unicamente quando è prevista da una norma di legge o di regolamento, non trovando perciò applicazione gli artt. 19, comma 2 e 39 del Codice (*Note* 1 ottobre e 28 gennaio 2011).

Una direzione didattica ha comunicato l'intenzione di trasmettere l'elenco nominativo degli insegnanti, bambini e altri operatori transitati presso l'istituto a partire dal 2000, all'azienda sanitaria locale, che ne aveva fatto richiesta per interventi di sanità pubblica, divenuti necessari in seguito al decesso di due bambini iscritti alla scuola elementare.

In merito, è stato rappresentato che tale operazione configura una comunicazione di dati personali non sensibili tra due soggetti pubblici, ammissibile se prevista da una norma (art. 19, comma 2, del Codice). In particolare, le norme di settore attribuiscono alle aziende sanitarie funzioni di vigilanza in merito all'igiene e alla medicina scolastica negli istituti di istruzione (artt. 14 e 20, l. 23 dicembre 1978, n. 833), nonché la promozione di azioni volte a rimuovere le cause di malattia di origine anche umana (artt. 7-*bis*, 7-*ter*, 7-*quater*, 7-*septies*, d.lgs. 30 dicembre 1992, n. 502).

Pertanto, nel rispetto dei princìpi di pertinenza e non eccedenza dei dati in relazione alle finalità del trattamento perseguite (art. 11 del Codice), in applicazione alle citate disposizioni legislative non è necessaria alcuna comunicazione preventiva al Garante (*Nota* 23 marzo 2010).

Ad un comune, che a seguito di una totale revisione della toponomastica e della numerazione civica, intendeva trasmettere i dati dei cittadini residenti a taluni soggetti pubblici e privati designandoli a tal fine "*responsabili del trattamento*", è stato precisato che non è necessaria alcuna comunicazione al Garante se sussiste una norma che preveda espressamente l'attivazione del flusso di dati (come nel caso della trasmissione di liste di dati anagrafici ai soggetti pubblici ai sensi dell'art. 34, comma 1, d.P.R. n. 223/1989), o se il soggetto privato destinatario venga designato responsabile del trattamento (art. 29 del Codice) (*Nota* 26 aprile 2010).

Nel caso di un altro comune che intendeva trasmettere ad una società di rilevazione dei consumi idrici i dati personali contenuti nelle banche dati anagrafiche, dei contribuenti TARSU/TIA e ICI, nonché il catasto terreni e fabbricati, è stato fatto presente che la comunicazione di dati personali da parte dei soggetti pubblici a privati è regolata da un distinto e più stringente quadro normativo (art. 19, comma 3, del Codice) (*Nota* 10 dicembre 2010).

In un altro caso, al comune che aveva chiesto chiarimenti in ordine alla legittimità del rifiuto opposto da un altro comune a una richiesta volta a conoscere determinate informazioni riguardanti una propria dipendente, è stato fatto presente che non risulta sindacabile da parte del Garante il diniego opposto dall'amministrazione interpellata in materia di accesso agli atti amministrativi né il diniego fondato sul combinato disposto degli artt. 19, comma 2, e 39 del Codice (*Nota* 11 giugno 2010).

3.8. L'ATTIVITÀ GIUDIZIARIA

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2010 sono pervenute segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 1° maggio 2005, n. 80), che prevede la pubblicazione, in appositi siti Internet, di copia dell'ordinanza del giudice che dispone sulla vendita forzata, nonché della relazione di stima dei beni da espropriare.

In riscontro a tali segnalazioni, l'Autorità ha richiamato il *provvedimento* 7 febbraio 2008 ([doc. *web* n. 1490838]; v. *Relazione* 2007, p. 55) con il quale ha indicato all'autorità giudiziaria e ai professionisti incaricati delle vendite l'esigenza di omettere nelle copie pubblicate sia dell'avviso di vendita, sia delle ordinanze e delle relazioni di stima, le generalità e ogni altro dato personale idoneo a rivelare l'identità del debitore e di eventuali soggetti terzi non previsto dalla legge e comunque non pertinente rispetto alla procedura in corso.

In un caso particolare l'interessato, di età avanzata, ha lamentato che la pubblicazione in Internet della consulenza tecnica d'ufficio riguardante una procedura esecutiva a lui relativa consentiva la sua agevole identificazione, in quanto non erano stati oscurati il luogo e la data di nascita del medesimo, unica persona nata in quel comune in quel giorno. Nel caso di specie l'Autorità, dopo aver verificato l'esattezza delle indicazioni contenute

nella segnalazione, ha ritenuto che, nonostante fosse stato omesso il nominativo dell'interessato, le informazioni pubblicate in chiaro nella consulenza tecnica ne consentissero effettivamente l'agevole identificazione. Tenuto conto delle peculiari circostanze della fattispecie, ha quindi invitato il giudice dell'esecuzione a disporre l'integrale oscuramento delle informazioni relative al segnalante (*Nota* 20 luglio 2010).

È pervenuta una segnalazione anche con riferimento alla pubblicazione su un quotidiano di un avviso recante i nominativi delle persone proprietarie di immobili confinanti con quello oggetto della procedura esecutiva. Nel riscontrare la segnalazione l'Autorità, ricordato il contenuto del *provvedimento* 7 febbraio 2008, ha provveduto a richiamare l'attenzione del giudice dell'esecuzione sul necessario rispetto dei princìpi posti a tutela della riservatezza sia dei soggetti coinvolti in procedimenti esecutivi, sia di eventuali soggetti terzi (*Nota* 5 maggio 2010).

In entrambi i casi le autorità giudiziarie hanno provveduto all'oscuramento delle informazioni oggetto delle segnalazioni.

3.8.1. L'informatica giuridica

Linee-guida per la diffusione dei provvedimenti giudiziari

A seguito di numerosi quesiti e segnalazioni, e dopo avere un'ampia consultazione con gli operatori e gli editori del settore, il Garante ha adottato, in data 2 dicembre 2010, le "*Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica*" ([doc. *web* n. 1774813], in *G.U.* 4 gennaio 2011, n. 2).

Le linee-guida attengono esclusivamente alla pubblicazione delle sentenze e dei provvedimenti giurisdizionali su riviste giuridiche, *cd-rom*, *dvd*, siti istituzionali, a fini di informazione giuridica. Non incidono, quindi, sulle norme processuali, quali quelle in materia di copie originali delle sentenze e degli altri provvedimenti giurisdizionali, o del loro deposito nelle cancellerie giudiziarie, e non riguardano l'attività giornalistica, che è oggetto di specifiche disposizioni (art. 136 ss. del Codice; "*Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica*", adottato dal Garante il 29 luglio 1998, in *G.U.* 3 agosto 1998, n. 179).

Con la *deliberazione*, viene prescritto l'obbligo di oscurare, sempre e in ogni caso, i dati dei minori e delle parti nei procedimenti che hanno ad oggetto i rapporti di famiglia e lo stato delle persone (ad es., controversie in materia di matrimonio, filiazione, adozione, abusi familiari, richieste di rettificazione di sesso), anche quando il giudizio si riferisca ad aspetti patrimoniali o economici. Devono, inoltre, essere omessi i dati relativi ad altre persone dai quali possa desumersi, anche indirettamente, l'identità dei soggetti tutelati. I dati devono essere oscurati non solo nei provvedimenti riprodotti per esteso, ma anche in quelli diffusi sotto forma di massima o contenuti in un elenco.

Al di fuori dei casi sopra indicati, nei quali la tutela opera *ope legis*, qualunque interessato (ad es., le parti in un giudizio civile o l'imputato in un processo penale, o anche un testimone o un consulente), può rivolgere un'istanza al giudice, prima della conclusione del processo, per chiedere che, in caso di riproduzione del provvedimento per finalità di informazione giuridica, siano oscurati le generalità e ogni altro elemento in grado di identificarlo. L'istanza deve indicare i "*motivi legittimi*" che la giustificano: ad es., la delicatezza del caso o la particolare natura dei dati contenuti nel provvedimento (stato di salute, vita sessuale). Se l'istanza è accolta si appone una annotazione sull'originale della sentenza.

L'anonimizzazione del provvedimento giudiziario 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).

Viene rilevato, infine, che non spetta all'ufficio giudiziario, ma a chi riceve la copia dei provvedimenti con l'annotazione che dispone l'oscuramento delle generalità provvedere in tal senso ove intenda riprodurli o diffonderli, anche sotto forma di massima, per finalità di informazione giuridica.

3.8.2. Trattamento di dati negli uffici giudiziari

Accertamenti presso il Consiglio di Stato e il TAR del Lazio

Con *provvedimento* 3 dicembre 2009, a seguito di una segnalazione ricevuta, il Garante ha deliberato di effettuare, ai sensi dell'art. 160 del Codice, gli accertamenti necessari a

verificare l'attuazione e l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia, ai sensi dell'art. 47, comma 2, del Codice, presso il Consiglio di Stato e il Tribunale amministrativo regionale del Lazio [doc. *web* n. 1753845].

Dalle verifiche svolte, pur in un generale quadro di rispetto delle regole, sono emerse alcune criticità. Il Garante ha pertanto prescritto alcune misure volte a rafforzare le misure di sicurezza a protezione dei dati trattati dai due uffici giudiziari sia in via informatica, sia in forma cartacea (*Provv.* 23 settembre 2010 [doc. *web* n. 1753845]).

Sotto il primo profilo, particolare attenzione è stata posta alla messa in sicurezza del Nuovo sistema informativo della giustizia amministrativa (NSIGA), che gestisce i documenti e i processi lavorativi dell'intero sistema, costituito dal Consiglio di Stato e dai ventinove Tribunali amministrativi regionali.

Deve essere in particolare garantito che per le comunicazioni gestite da NSIGA fra le sedi del sistema giudiziario amministrativo e per gli accessi dei magistrati a NSIGA da postazioni esterne agli uffici –la *cd.* "*scrivania del magistrato*"– sia adottato un protocollo che cifri i dati in transito. Tutte le operazioni compiute su NSIGA dai magistrati e dal personale amministrativo devono essere tracciate, compresi gli accessi in sola lettura e non solo le operazioni di scrittura. Devono, inoltre, essere adottate delle *policy* che specifichino agli utenti di non utilizzare *password* banali per accedere a NSIGA (ad es., contenenti il nome stesso dell'utente).

Infine, l'accesso alla sala *server* e alla sala dove sono collocati i gruppi di continuità deve essere registrato (tramite *log*) e consentito solo con *badge* nominativi. I locali, inoltre, devono essere costantemente monitorati, eventualmente anche attraverso un impianto di videosorveglianza interno.

Quanto al trattamento in via cartacea, il Consiglio di Stato deve custodire i fascicoli processuali in armadi tutti dotati di serratura e il TAR del Lazio deve collocare i fascicoli dell'archivio in locali chiusi e controllati.

Sia il Consiglio di Stato che il TAR del Lazio hanno comunicato di aver già posto in essere gran parte delle misure indicate.

Accesso ad atti giudiziari

Sono giunti al Garante alcuni quesiti posti da uffici giudiziari in materia di accesso ad atti concernenti i processi. In un caso, una testata televisiva giornalistica aveva chiesto di accedere agli atti di un processo penale, al fine di utilizzare il materiale nell'ambito di un programma avente ad oggetto vicende giudiziarie. In un altro caso, un avvocato privo di mandato difensivo aveva chiesto di prendere visione dei ruoli di udienza.

Nel fornire riscontro, l'Autorità ha in primo luogo ricordato che la normativa in materia di protezione dei dati personali non ha innovato o modificato la disciplina relativa alla conoscenza degli esiti e dei calendari dei processi –come alla visione e al rilascio di estratti e di copie di atti giudiziari, alla pubblicità delle udienze e alla consultazione dei registri relativi ai procedimenti giudiziari– che rimane assoggettata alle pertinenti disposizioni processuali (art. 51 del Codice). Si tratta di attività che integrano trattamenti svolti "*per ragioni di giustizia*" (art. 47, comma 2, del Codice), che vengono svolte sotto il controllo dell'autorità giudiziaria e nel rispetto delle norme di settore. La decisione in ordine all'accesso deve essere quindi ricavata nel quadro del regime di pubblicità attribuito agli atti dalle norme processuali.

In secondo luogo, l'Autorità ha, peraltro, rilevato che anche a tali trattamenti si applicano i princìpi posti dall'art. 11 del Codice, in base ai quali l'accesso ai dati personali può essere consentito solo previa verifica dell'esistenza di uno scopo determinato, esplicito e legittimo (comma 1, lett. *b*)) e relativamente alle sole informazioni pertinenti e non eccedenti rispetto allo scopo medesimo (comma 1, lett. *d*)).

In caso di decisione favorevole a consentire l'accesso, il Garante ha, infine, invitato l'autorità giudiziaria a valutare attentamente la possibilità di raggiungere gli scopi perseguiti dal soggetto richiedente sulla base di soli dati anonimi, mediante preventiva omissione di informazioni atte a consentire l'identificazione dei soggetti coinvolti nei giudizi (*Note* 5 gennaio e 21 gennaio 2011).

3.8.3. Notificazioni di atti e comunicazioni

Come negli anni precedenti, il Garante è intervenuto in numerose occasioni per assicurare l'adozione di procedure idonee a tutelare la riservatezza delle persone alle quali

vengono notificati atti giudiziari, verbali di contravvenzione, avvisi fiscali o altri atti amministrativi (art. 174 del Codice).

In particolare, con riferimento alle notificazioni di atti tributari, l'Ufficio ha ricordato che sulla busta devono essere leggibili solo le informazioni necessarie all'invio della comunicazione al destinatario (art. 11, comma 1, del Codice) (*Nota* 28 aprile 2010).

In un'altra occasione è stato evidenziato che la notificazione deve essere effettuata in busta sigillata solo se la consegna non possa avvenire nelle mani proprie del destinatario al quale l'atto può essere notificato, ancorché aperto, per il tramite del messo comunale. Con particolare riferimento all'accessibilità del contenuto del documento da parte degli addetti al protocollo e del messo comunale, si è precisato che essi, in qualità di dipendenti pubblici ovvero incaricati di pubblico servizio, sono tenuti al segreto d'ufficio (art. 15 del d.P.R. 20 gennaio 1957, n. 3) (*Nota* 13 maggio 2010).

4. La sanità

4.1. Il trattamento di dati idonei a rivelare lo stato di salute

4.1.1. I trattamenti per fini di cura della salute

Anche nel 2010, l'Autorità ha richiamato l'attenzione dei titolari del trattamento operanti in ambito sanitario sulla necessità di fornire l'informativa e di acquisire il consenso per il trattamento dei dati personali nell'ambito del rapporto medico paziente.

Al riguardo sono stati forniti chiarimenti in ordine alle modalità di acquisizione del consenso di minori detenuti temporaneamente nei centri di prima accoglienza, in caso di assenza di chi ne esercita legalmente la potestà genitoriale; è stato in particolare evidenziato che è possibile acquisire il consenso, in tale caso, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora (art. 82, comma 2, lett. *a*), del Codice) (*Nota* 30 settembre 2010).

Merita altresì menzione una segnalazione circa l'illegittima acquisizione, da parte del coniuge del segnalante, di alcuni scritti contenuti in un diario, successivamente consegnati ad un medico specialista per la redazione di un parere sullo stato di salute del segnalante, poi prodotto nel giudizio di separazione.

In merito è stato rappresentato che la validità, l'efficacia e l'utilizzabilità in giudizio di atti, basati sul trattamento di dati non conforme alle norme vigenti restano disciplinate dalle pertinenti disposizioni processuali (art. 160, comma 6, del Codice; cfr. *Provv.* 23 settembre 2010 [doc. *web* n. 1756065]) e che resta salva la facoltà della persona interessata di far valere le proprie pretese risarcitorie, ove ne ricorrano i presupposti, davanti all'autorità giudiziaria ordinaria (art. 15 del Codice) (*Nota* 22 ottobre 2010).

4.1.1.1. Le linee-guida in tema di fascicolo sanitario elettronico (FSE) e di dossier *sanitario*

Una regione ha sottoposto al Garante uno schema di regolamento in materia di fascicolo sanitario elettronico e di *dossier* sanitario elettronico.

Al riguardo, l'Ufficio ha ricordato che, in base alle "*Linee-guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario*" (*Provv.* 16 luglio 2009 [doc. *web*

n. 1634116]), i trattamenti di dati personali effettuati attraverso il FSE devono essere resi noti al Garante mediante una apposita comunicazione da effettuarsi secondo il modello adottato dall'Autorità con specifico *provvedimento* (*Provv.* 16 luglio 2009 [doc. *web* n. 1633793]), da parte delle strutture coordinatrici delle iniziative di FSE e, in via residuale, in caso di assenza di tale struttura, dai singoli titolari del trattamento coinvolti.

La suddetta comunicazione non deve essere effettuata nel caso di *dossier* sanitari e dall'invio di tali comunicazioni non può desumersi alcuna approvazione implicita da parte dell'Autorità delle iniziative comunicate (*Nota* 26 luglio 2010).

Ad oggi risultano pervenute 44 comunicazioni, delle quali solo 6 effettivamente riconducibili al FSE, mentre le altre non dovevano essere inviate in quanto relative ad altri trattamenti (ad es., *dossier* sanitari; condivisione da parte di più strutture solo di alcuni dati clinici del paziente e non della sua intera storia clinica; flussi di dati per finalità amministrative correlate alla cura; flussi di dati tra aziende sanitarie e medici di medicina generale; trattamenti effettuati da farmacie nell'ambito della somministrazione di farmaci).

4.1.1.2. Consultazione online *dei referti medici*

È stato chiesto dal Ministero della salute il previsto parere al Garante su uno schema di decreto di attuazione delle disposizioni che hanno definito nuovi compiti e funzioni assistenziali per le farmacie pubbliche e private convenzionate con il servizio sanitario nazionale (art. 1, comma 2, lett. *f*), d.lgs. 3 ottobre 2009, n. 153), tra cui la prenotazione di prestazioni ambulatoriali presso le strutture accreditate, i relativi pagamenti, ed il ritiro dei referti. Lo schema di decreto ha sostanzialmente recepito le indicazioni rese dall'Autorità per garantire un più elevato *standard* di tutela del diritto alla protezione dei dati personali. Tuttavia, è stata evidenziata l'esigenza che al momento del ritiro del referto da parte degli assistiti presso le farmacie, l'operatore acceda al referto stesso solo per consegnarlo all'interessato, e che sia impedita la creazione di banche dati di referti digitali presso la farmacia (*Parere* 19 gennaio 2011 [doc. *web* n. 1787887]).

Nell'ambito dello stesso parere è stata altresì rappresentata l'esigenza di individuare adeguati tempi di conservazione dei referti (art. 11, comma 1, lett. *e*), del Codice) e che

gli operatori della farmacia, individuati quali incaricati del trattamento dei dati nell'ambito del sistema CUP (centro unificato di prenotazione), non tenuti per legge al segreto professionale, siano sottoposti a regole di condotta analoghe al segreto professionale, come già previsto in ambito sanitario (art. 83, comma 2, lett. *i*), del Codice).

4.1.2. I trattamenti per fini amministrativi

In diverse occasioni, l'Ufficio ha ricordato alle strutture sanitarie che per perseguire finalità amministrative correlate alle finalità di cura non devono acquisire il consenso dell'interessato, ma rispettare i limiti e le garanzie individuate nei regolamenti regionali adottati in conformità allo schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e di altri enti, su cui il Garante ha espresso parere favorevole (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

Da parte di più enti, anche alla luce delle numerose modifiche normative sopravvenute, è stata manifestata l'esigenza di revisionare il predetto schema-tipo di regolamento, ed a tal fine, l'Ufficio, che ha condiviso tale necessità, partecipa ad un tavolo di lavoro interregionale all'uopo istituito.

Tra i casi di maggior rilievo affrontati, si evidenziano talune segnalazioni relative al trattamento da parte di un comune, di dati idonei a rivelare lo stato di salute di cittadini, contenuti in prescrizioni mediche di farmaci svizzeri e in documenti relativi alla avvenuta dispensazione di tali farmaci.

Il comune, nel fornire riscontro alla richiesta di informazioni dell'Ufficio, aveva documentato di essere stato legittimato al trattamento, in quanto designato responsabile del trattamento di dati personali da parte della azienda sanitaria, sicché l'istruttoria preliminare si è conclusa senza specifici provvedimenti del Garante (v. artt. 11, comma 1, lett. *d*) e 13, comma 4, del regolamento del Garante n. 1/2007) (*Note* 15 dicembre 2010) (v. anche il parere favorevole del Garante sullo schema-tipo di regolamento per il trattamento dei dati sensibili e giudiziari effettuato dai comuni *Provv.* 21 settembre 2005 [doc. *web* n. 1170239]).

Nel riscontrare, infine, talune osservazioni sullo svolgimento di attività connesse al servizio CUP, da parte di detenuti di una casa di reclusione, l'Ufficio ha confermato che, se designati

incaricati del trattamento, i detenuti possono legittimamente trattare dati personali di cui l'azienda sanitaria è titolare per lo svolgimento delle sue funzioni istituzionali. Gli incaricati del trattamento devono operare sotto la diretta autorità del titolare o del responsabile e attenersi alle istruzioni loro impartite (art. 30 del Codice) (*Nota* 1 luglio 2010).

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

L'Autorità ha nuovamente affrontato la questione relativa alla comunicazione, adottando un *provvedimento* di divieto di comunicazione dei dati relativi ai risultati degli accertamenti diagnostici diretti o indiretti per l'infezione da *HIV*, a persona diversa dall'interessato.

In particolare, un cittadino aveva lamentato di essere stato informato del suo stato di sieropositività dal medico di famiglia, il quale ne aveva avuto notizia da un medico operante presso la casa di cura ove erano state effettuate le analisi per l'accertamento dell'infezione da *HIV*.

Al riguardo, considerato l'obbligo di comunicare i risultati di tali esami esclusivamente alla persona cui essi sono riferiti (art. 5, comma 4, l. 5 giugno 1990, n. 135), il Garante ha vietato non solo alla casa di cura, ma anche al medico di famiglia del segnalante che aveva indebitamente avuto notizia dei risultati, la comunicazione dei predetti dati a persona diversa dall'interessato (*Provv.* 27 maggio 2010 [doc. *web* n. 1738383]).

In relazione ad un quesito presentato da un ordine dei medici, in ordine alla raccolta di dati personali relativi allo stato di sieropositività dei pazienti che si rivolgono per la prima volta ad uno studio medico, l'Ufficio ha chiarito che quanto prescritto nei *provvedimenti* 12 novembre 2009 [doc. *web* nn. 1686068 e 1673588] non ha in alcun modo inteso impedire la raccolta di dati anamnestici del paziente. Nei citati provvedimenti, infatti, l'Autorità ha espressamente evidenziato che la doverosa raccolta da parte del medico di un'anamnesi dettagliata non può impedire all'interessato di scegliere, in modo informato –e quindi consapevole– di non comunicare al medico alcune informazioni sanitarie che lo riguardano, ivi compresa la sua eventuale sieropositività, senza perciò subire alcun pregiudizio sulla possibilità di usufruire delle prestazioni sanitarie richieste

(cfr. par. n. 3, linee-guida in tema di fascicolo sanitario elettronico (FSE) e di *dossier* sanitario - *Provv.* 16 luglio 2009 [doc. *web* n. 1634116]).

Nella medesima occasione è stato, inoltre, puntualizzato che contrasta con i princìpi di pertinenza e non eccedenza dei dati rispetto alle finalità di cura dell'interessato, la raccolta di informazioni sull'eventuale stato si sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, effettuata in fase di accettazione, indipendentemente dal tipo di intervento clinico o dal piano terapeutico che lo stesso deve eseguire (ad es., trattamento di igiene orale professionale, ablazione del tartaro, *rx* ortopanoramica). Tali informazioni –previo consenso informato del paziente– possono infatti essere raccolte solo se necessarie in funzione del tipo di intervento sanitario o di piano terapeutico.

Sempre con riferimento ai dati relativi all'accertamento dell'infezione da *HIV*, l'Ufficio ha, altresì, avviato una istruttoria a seguito di una notizia stampa, in ordine allo svolgimento di indagini sanitarie volte ad accertare l'esistenza dell'infezione da *HIV*, tra i dipendenti di una azienda sanitaria, chiedendo ogni elemento di valutazione in ordine a quanto riportato nell'articolo, specie con riferimento al rispetto delle specifiche disposizioni contenute nella l. n. 135/1990 (*Nota* 30 novembre 2010).

4.1.4. Le strutture sanitarie e la tutela della dignità delle persone

Come già avvenuto nel corso degli ultimi anni, il Garante ha richiamato al rispetto delle misure previste dal Codice a tutela della dignità della persona in ambito sanitario (art. 83), numerosi organismi sanitari pubblici e privati, che hanno di conseguenza modificato le modalità di erogazione previste per la fornitura delle prestazioni e dei servizi sanitari.

Si menziona in proposito una segnalazione effettuata durante un servizio giornalistico televisivo, dalla quale era emerso che un ospedale sardo non aveva rispettato, in particolare, la dignità e la riservatezza di una paziente in stato comatoso.

Al riguardo, l'Ufficio ha richiamato al rispetto della dignità dei pazienti sottoposti a trattamenti medici invasivi, o nei cui confronti è comunque doverosa una specifica attenzione (v. punto 3, lett. *a*), del *Provv.* generale 9 novembre 2005 [doc. *web* n. 1191411] sul rispetto della dignità degli interessati nelle strutture sanitarie) (*Nota* 10 maggio 2010).

L'ospedale ha comunicato di aver previsto idonee misure, anche di tipo organizzativo, volte a progettare gli spazi disponibili, in modo da renderli più rispettosi dei diritti dei malati.

È stato, inoltre, segnalato che la prenotazione di prestazioni sanitarie e il pagamento del *ticket* presso il centro unificato di prenotazione (CUP) di un ospedale umbro venivano effettuati con modalità tali da consentire la conoscenza di dati sensibili degli interessati da parte di altri soggetti a causa della mancanza di appropriate distanze di cortesia.

Interpellato sul punto, l'ospedale ha comunicato di aver posto in essere taluni accorgimenti idonei a garantire la riservatezza degli interessati, tra i quali la predisposizione di apposite distanze di cortesia per coloro che effettuano la prenotazione di prestazioni sanitarie, e la previsione di specifiche modalità per informare i terzi legittimati sulla dislocazione dei degenti nei reparti (art. 83, comma 2, lett. *c*) e *d*), del Codice; punto 3, lett. *b*), del cit. *provvedimento*) (*Nota* 12 marzo 2010).

Anche un servizio di igiene e sanità pubblica, richiamato dal Garante in ordine alla necessità di adottare misure idonee a garantire la riservatezza di una minore, in occasione delle chiamate per effettuare la vaccinazione ed acquisire il consenso informato dei genitori, ha comunicato di voler istituire una procedura di chiamata alfanumerica al momento dell'accettazione (*Nota* 7 dicembre 2010).

In relazione ad una segnalazione relativa alla "*poca attenzione*" posta nella conservazione delle cartelle cliniche dei pazienti, in una casa di cura pugliese, l'Ufficio ha rappresentato alla menzionata struttura sanitaria che il titolare del trattamento deve adottare procedure idonee a garantire la custodia di atti e documenti in archivi ad accesso selezionato (art. 35 del Codice) e che qualora gli atti o i documenti contengano dati personali sensibili, gli stessi devono essere controllati e custoditi dagli incaricati durante lo svolgimento dei relativi compiti fino alla loro restituzione, in maniera che agli stessi non possano accedere persone prive di autorizzazione (punto 28 del Disciplinare tecnico Allegato B. al Codice).

Essendo emerso dall'istruttoria preliminare, in particolare, che il trattamento dei dati contenuti in taluni referti radiologici non era conforme alle misure minime di sicurezza

prescritte dal Codice (artt. 33-36 del Codice e Allegato B. al Codice), la casa di cura ha assicurato di aver provveduto a garantire la custodia di atti e documenti in archivi ad accesso selezionato, in particolare, sistemando i citati referti in appositi armadi chiusi e custoditi da personale sanitario (*Nota* 23 novembre 2010).

Sulla base di una notizia di stampa, relativa ad un policlinico all'interno del quale, presso taluni cassonetti per la raccolta dei rifiuti era stata abbandonata documentazione clinica, unitamente a documenti contabili riguardanti pazienti della struttura, l'Ufficio ha riscontrato, la non conformità del trattamento alle misure minime di sicurezza prescritte dal Codice (artt. 33-36 del Codice e Allegato B. al Codice) (*Nota* 13 dicembre 2010).

In un'altra segnalazione si lamentava la comunicazione, ad un familiare che ne aveva fatto richiesta, dei nominativi di tutti i soggetti residenti presso una casa di riposo che erano stati trasportati presso gli ospedali della zona per visite e accertamenti sanitari, e non soltanto del singolo parente.

Nel riscontrare le specifiche richieste di chiarimenti dell'Ufficio, la casa di riposo si è impegnata, qualora si ripresentasse una simile richiesta, a fornire dati anonimi, per quel che riguarda i soggetti diversi dal familiare, in modo da evitare la ripetizione della condotta lamentata.

Alla luce delle idonee assicurazioni fornite, non sono stati adottati specifici provvedimenti da parte del Garante (art. 11, comma 1, lett. *d*) e 13, comma 4, del regolamento n. 1/2007) (*Nota* 11 giugno 2010).

Su un altro piano, merita particolare attenzione un parere reso alla Presidenza del Consiglio dei ministri-Commissione per l'accesso ai documenti amministrativi.

Nella vicenda un genitore, avendo trovato nella camera della figlia sedicenne una confezione di un farmaco contraccettivo già utilizzato, aveva chiesto all'azienda sanitaria di zona di accedere ai documenti sanitari più recenti della minore per assicurarsi, a suo dire, che il farmaco fosse stato prescritto da personale medico.

Nel parere, l'Autorità ha condiviso quanto affermato dalla Commissione secondo la quale, in base alla l. 22 maggio 1978, n. 194, i minori possono rivolgersi alle aziende ospedaliere e ai consultori senza che i genitori ne siano informati in quanto, l'obiettivo

della norma è quello di garantire l'anonimato dei minorenni che non vogliano o non possano mettere al corrente i propri genitori, ed evitare che le minori possano rivolgersi clandestinamente a soggetti privi della necessaria affidabilità, serietà e professionalità invece che a strutture sanitarie autorizzate, in grado di assicurare le necessarie garanzie (*Parere* 17 novembre 2010 [doc. *web* n. 1769451]).

4.1.5. La ricerca scientifica

Nel corso dell'anno l'Autorità ha in più di un caso autorizzato il trattamento di dati relativi allo stato di salute degli interessati, in mancanza del loro consenso, a fini di ricerca scientifica in campo medico ed epidemiologico (art. 110 del Codice). Le autorizzazioni sono state accordate in ragione della rilevanza degli scopi scientifici perseguiti, nonché delle difficoltà, rappresentate nei diversi casi, di informare i pazienti per acquisire il loro consenso, trattandosi di studi retrospettivi relativi a cospicui campioni di interessati, spesso irreperibili.

In tutti i casi è stato autorizzato il trattamento delle sole informazioni indispensabili per lo svolgimento degli studi, e sono state individuate le precauzioni nel curare ed incrementare il livello di sicurezza del trattamento dei dati in conformità alle "*Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali*" (*Provv.* 24 luglio 2008 [doc. *web* n. 1533155].

Più in dettaglio, con un *provvedimento* (27 aprile 2010 [doc. *web* n. 1722683]) un'università francese è stata autorizzata ad accedere alla documentazione medico-clinica di un campione di circa 3.000 pazienti italiani con insufficienza epatica acuta, per uno studio retrospettivo di farmacoepidemiologia che coinvolgeva i centri trapianti di 7 Paesi europei, volto ad individuare i potenziali rischi per la salute derivanti da farmaci antinfiammatori contenenti una determinata sostanza attiva.

Lo studio era stato raccomandato dall'Agenzia europea per i medicinali, ed alla sua realizzazione era stato subordinato, dalla Commissione europea, il mantenimento delle autorizzazioni all'immissione in commercio (cfr. art. 133 d.lgs. del 24 aprile 2006, n. 219).

Il *provvedimento* di autorizzazione ha però prescritto che, qualora i pazienti dovessero

tornare a rivolgersi ai centri trapianti, dovranno essere informati sul trattamento dei loro dati e dovrà essere richiesto il loro eventuale consenso.

Un'altra autorizzazione (*Provv.* 16 settembre 2010 [doc. *web* n. 1753153]) è stata rilasciata ad una casa farmaceutica, promotrice di uno studio clinico sul tumore alla mammella, ad un'azienda ospedaliera, quale centro di ricerca coordinatore, e ad altri 48 centri di cura, per accedere alla documentazione medico-clinica di un campione di 1.000 pazienti curate presso gli stessi centri, in assenza del consenso al trattamento dei dati di coloro che, al momento dell'arruolamento, risultassero irreperibili o decedute, a seguito di apposite verifiche effettuate dal personale medico dei centri partecipanti.

Lo studio, prevedeva di raccogliere retrospettivamente i dati clinici delle pazienti che avevano iniziato il trattamento nel 2007, quando alcuni farmaci non erano in uso, per confrontarli con quelli delle pazienti sottoposte nel 2009-2010 alle nuove terapie in esame.

L'autorizzazione prevede che i nominativi delle donne, siano trattati esclusivamente dai centri di cura preposti, nella sola fase di individuazione del campione e di raccolta dei dati sanitari dalle cartelle cliniche, mentre nelle fasi successive dello studio, a partire dalla registrazione dei dati, questi siano sostituiti con un codice identificativo univoco associato ai singoli centri. Una volta concluso lo studio, i dati raccolti vanno trasformati in forma anonima.

Per garantire, a partire dalla fase di registrazione dei dati, la loro protezione dai rischi di accesso non autorizzato o di trattamento non consentito, è stato indicato anche il ricorso a tecnologie crittografiche. Inoltre, con riferimento al *database* centralizzato per l'archiviazione dei dati dello studio devono essere previsti sistemi di *audit log* in grado di garantire la loro inalterabilità, al fine di assicurare il controllo degli accessi al *database* e il rilevamento di eventuali anomalie.

Un'altra autorizzazione è stata rilasciata all'Istituto superiore di sanità, per il trattamento dei dati personali riguardanti le donazioni effettuate e le trasfusioni ricevute da soggetti segnalati al Registro della malattia di *Creutzfeldt-Jacob* e sindromi correlate, per uno studio epidemiologico retrospettivo sul rischio di trasmissione della forma sporadica della malattia attraverso le trasfusioni di sangue o di suoi derivati. Lo studio prevede, in

particolare, di raccogliere i dati personali e sanitari dei donatori di sangue a pazienti inseriti nel Registro, nonché dei riceventi trasfusioni dai medesimi pazienti presso i centri di coordinamento regionale sangue e le strutture trasfusionali periferiche, tramite la collaborazione del Centro nazionale sangue, nonché presso le aziende sanitarie di residenza degli interessati.

In particolare, l'Istituto aveva evidenziato l'impossibilità, per motivi etici, di informare i donatori o i trasfusi di soggetti segnalati al Registro della malattia di *Creutzfeldt-Jacob* e sindromi correlate, in quanto ciò li avrebbe portati a conoscenza del rischio di sviluppare in futuro la stessa malattia incurabile e fatale, rischio peraltro non ancora accertato e che lo studio mirava proprio a definire e a quantificare.

Nell'autorizzazione, il Garante ha rilevato che, per le sue caratteristiche, lo studio non avrebbe potuto essere realizzato mediante il trattamento di dati anonimi, né senza l'identificazione, anche temporanea, degli interessati (*Provv.* 4 novembre 2010 [doc. *web* n. 1767796]).

Sempre nel corso dell'anno, in applicazione dell'art. 105, comma 4, del Codice e dell'art. 6, comma 4, del codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici, sono state individuate le modalità per l'informativa, da parte dell'Istituto superiore di sanità, in collaborazione con il Ministero della difesa, da rendere per la realizzazione del Progetto di sorveglianza epidemiologica dei tumori nella popolazione militare impegnata in Bosnia-Herzegovina e nel Kosovo –ove è stato fatto uso di uranio impoverito– incluso nel programma nazionale per la ricerca sanitaria di cui all'art. 12-*bis* del d.lgs. n. 502/1992. Il progetto prevede la realizzazione di due studi retrospettivi volti a verificare la mortalità e l'incidenza di tumori nei membri di due coorti formate dai militari inviati in missione nei medesimi territori dal 1995 al 2004 e da un campione di carabinieri, mai impegnati in teatri operativi all'estero.

Ritenendo che il conferimento dell'informativa a ciascun interessato, ai sensi dell'art. 13 del Codice, avrebbe richiesto uno sforzo sproporzionato rispetto al diritto tutelato, il Ministero della difesa ha quindi informato l'Autorità di voler pubblicare l'informativa su due quotidiani di diffusione nazionale, sui siti Internet del Ministero della difesa, delle

singole forze armate e delle associazioni del personale in quiescenza, su riviste e pubblicazioni militari diffuse anche tra il personale in servizio e su circolari destinate alle strutture centrali e periferiche delle stesse forze armate.

Il Garante, anche in relazione all'ingente numero di persone interessate ed alla mancanza di informazioni utili a raggiungerle, per garantire la più ampia conoscibilità di tale informativa, ha stabilito che essa sia pubblicata altresì sul sito Internet dell'Istituto superiore di sanità e che rimanga agevolmente reperibile e visibile ivi e sugli altri siti individuati dal Ministero della difesa fino alla conclusione del progetto (*Provv.* 19 gennaio 2011 [doc. *web* n. 1787877]).

In un altro caso è stato evidenziato che i trattamenti di dati sensibili effettuati dall'Agenzia regionale per la protezione ambientale, per la realizzazione di programmi di ricerca in campo epidemiologico approvati dalla Giunta regionale, in attuazione dell'art. 5, comma 4-*bis*, della l. Regione Marche 2 settembre 1997, n. 60, possono essere effettuati in conformità alla disciplina prevista dal Codice per i trattamenti a scopo di ricerca scientifica (artt. 20, 22, 107 e 110 del Codice) (*Nota* 20 maggio 2010).

5. I DATI GENETICI

Si è riferito nella *Relazione* 2009 (p. 117), sul nuovo schema di autorizzazione generale al trattamento di dati genetici, inviato al Ministero della salute per il parere del Consiglio superiore di sanità previsto dall'art. 90 del Codice. Nel parere, il Consiglio superiore di sanità ha formulato alcuni suggerimenti in ordine alle definizioni utilizzate dall'autorizzazione, all'individuazione degli ambiti della ricerca scientifica ed alle finalità di tutela della salute per i quali è autorizzato il trattamento di dati genetici.

L'Ufficio del Garante, all'esito di un doveroso approfondimento –anche alla luce dell'esperienza in ambito comunitario– delle indicazioni del Consiglio, riguardanti in particolare, la definizione di "dato genetico", ha modificato la formulazione proposta, al fine di evitare l'esclusione dal novero dei dati genetici delle informazioni relative alle caratteristiche genotipiche di un individuo che, pur non essendo il risultato di analisi genetiche, presentano alcune caratteristiche comuni ai dati genetici, tali da rendere opportuna la previsione di particolari cautele nel loro trattamento.

Sul punto, di particolare rilevanza, si è reso necessario acquisire un nuovo parere del Consiglio superiore di sanità (*Nota* 17 settembre 2010).

Nelle more del completamento di tali valutazioni, con *deliberazione* del 23 dicembre 2010 è stata ulteriormente prorogata l'efficacia della vigente autorizzazione generale sino al 30 giugno 2011, per permettere nel frattempo, alle medesime condizioni, la prosecuzione dei trattamenti di dati genetici già autorizzati (*Provv.* 23 dicembre 2010 [doc. *web* n. 1776159] in *G.U.* 4 gennaio 2011, n. 2).

Sul trattamento di dati genetici per finalità di ricerca statistica v. par. 6.

Sull'avvio, da parte del Gruppo europeo in materia di cooperazione giudiziaria e di polizia, dell'analisi dell'utilizzo dei dati genetici contenuti nelle banche dati *DNA* per finalità giudiziarie e di polizia v. par. 20.3.

6. La ricerca statistica e storica

Nel 2010 il Garante ha reso due pareri ai sensi dell'art. 6-*bis*, comma 2, del d.lgs. 6 settembre 1989, n. 322 (che disciplina, tra l'altro, il Sistema statistico nazionale): il primo sui prospetti identificativi di lavori statistici da inserire nell'aggiornamento 2010 del Programma statistico nazionale 2008-2010, il secondo sullo schema di Programma statistico nazionale 2011-2013 (*Parere* 10 giugno 2010 [doc. *web* n. 1734415]; *Parere* 23 settembre 2010 [doc. *web* n. 1753181]).

Nel parere 10 giugno 2010 il Garante ha ribadito considerazioni già espresse in precedenti occasioni: in particolare, l'ulteriore conservazione dei dati dopo la costituzione di un sistema informativo statistico deve considerarsi un'eccezione rispetto alla regola generale (v. *Parere* 24 settembre 2009 [doc. *web* n. 1657731]); ha ribadito altresì che l'inserimento di un campo contenente le fonti normative risulta necessario solo quando occorre informare gli interessati circa l'esistenza di una norma di legge o di regolamento che consenta la raccolta di dati sensibili e giudiziari indipendentemente dalla volontà dell'interessato di aderire alla ricerca (v. *Parere* 15 novembre 2007 [doc. *web* n. 1464806]).

Inoltre, la mancata individuazione di informazioni sensibili (quali l'adesione a partiti, sindacati, organizzazioni a carattere religioso) e giudiziarie nei prospetti identificativi, comporta l'impossibilità di trattare questi dati (v. *Parere* 22 ottobre 2008 [doc. *web* n. 1565063]).

Ancora, il trattamento di dati genetici (che può essere effettuato per fini statistici secondo le modalità e nei limiti dell'*autorizzazione* al trattamento dei dati genetici del 22 febbraio 2007 [doc. *web* n. 1389918]) va opportunamente evidenziato nei prospetti identificativi, anche per poter rendere agli interessati un'informativa completa.

L'Autorità ha, inoltre, rilevato che numerosi lavori statistici non solo non prevedono l'anonimizzazione dei dati dopo la raccolta, ma non garantiscono neanche la conservazione separata dei dati identificativi quando gli stessi, anche di carattere sensibile e giudiziario, sono conservati per ulteriori trattamenti statistici. Con riferimento all'ipotesi in cui l'impossibilità di conservare separatamente i dati identificativi derivi dal trattamento

amministrativo sottostante, il Garante ha precisato che in ogni caso i dati sensibili e giudiziari contenuti in elenchi, registri e banche dati devono essere resi momentaneamente inintelligibili anche a chi è autorizzato ad accedervi, permettendo l'identificazione degli interessati solo in caso di necessità; inoltre, i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali che non richiedono il loro utilizzo (art. 22, commi 6 e 7, del Codice).

Da ultimo, al fine di consentire la più ampia conoscibilità dei prospetti identificativi dei lavori statistici, il Garante ha manifestato di ritenere opportuna la pubblicazione del PSN nei siti Internet istituzionali dell'ISTAT, del Sistema statistico nazionale (SISTAN) e degli enti ed uffici di statistica che partecipano al SISTAN.

Con riferimento al PSN 2011-2013, l'ISTAT e l'Autorità hanno costituito un gruppo di lavoro misto, per definire gli elementi da inserire nei prospetti ai fini dell'informativa agli interessati, e per garantire un più elevato *standard* di tutela del diritto alla protezione dei dati personali (*Nota* 2 aprile 2010).

Il Programma statistico nazionale 2011-2013, contiene, infatti, numerose innovazioni tra le quali, il Garante ha valutato positivamente la scelta di rendere parte integrante dell'informativa semplificata, un paragrafo del PSN relativo alle "*caratteristiche generali dei lavori che trattano dati personali*", che non vengono, pertanto, ripetute in ogni singolo prospetto identificativo (*Parere* 23 settembre 2010 [doc. *web* n. 1753181]).

Nel parere da ultimo citato il Garante ha, in particolare, segnalato l'opportunità di compilare in maniera più omogenea, nei PSN futuri, i prospetti identificativi dei lavori statistici, per non ingenerare confusione negli interessati.

La Regione Liguria aveva chiesto il parere del Garante sul documento programmatico relativo alle "*elaborazioni statistiche dei dati di mortalità nell'ambito della 'Procedura sperimentale per l'acquisizione dei dati di mortalità'*", in relazione al trattamento di dati sensibili per un'elaborazione non inserita nel PSN.

Il Garante, rilevata la pertinenza delle informazioni e riconosciuta la possibilità che esse siano ulteriormente conservate per indagini continue e longitudinali, di controllo, di qualità e di copertura (cfr. art. 11 del Codice; art. 11 del codice di deontologia e di buona

condotta, Allegato A.3. al Codice), ha espresso parere favorevole condizionato, però, al rigoroso rispetto delle cautele ivi richiamate, sull'utilizzo di dati idonei a rivelare lo stato di salute degli interessati, anche contenuti in elenchi, registri e banche dati (*Parere* 23 settembre 2010 [doc. *web* n. 1753195]).

Un'università aveva comunicato di voler trasmettere alla richiedente camera di commercio industria artigianato e agricoltura, per un'indagine allo stato non rientrante nel programma statistico nazionale, i dati personali (tra cui le generalità, il tipo di corso di studio, i recapiti anche telefonici) dei laureati nell'anno 2005. L'Ufficio, rilevato che l'indagine è risultata riconducibile alle funzioni istituzionali della camera di commercio (art. 2, comma 2, lett. *n*), l. 29 dicembre 1993, n. 580) e che i trattamenti di dati personali per la produzione di informazione statistica non compresi nel PSN possono essere effettuati solo dall'Ufficio di statistica della camera di commercio, ha ritenuto che la suddetta comunicazione potesse essere effettuata. È stata però, evidenziata, in particolare, l'esigenza di un'idonea informativa agli interessati, per assicurare la volontarietà dell'adesione all'iniziativa; è stato altresì precisato che non possono essere trattati, in tale ambito, dati sensibili e giudiziari, soggetti a regole più rigide (artt. 20-22 del Codice; art. 6-*bis*, comma 2, d.lgs. 322 del 1989) (*Nota* 17 maggio 2010).

L'Agenzia delle entrate aveva effettuato una comunicazione al Garante, per trasmettere al richiedente Ufficio studi di una provincia alcuni dati relativi alle dichiarazioni prodotte dal sostituto d'imposta sul modello 770 per gli anni d'imposta 2003 e 2007, per un'analisi delle retribuzioni e della relativa dinamica. Anche in questo caso, trattandosi di informazione statistica non compresa nel Programma statistico nazionale, si è evidenziato che il trattamento poteva essere svolto esclusivamente dall'Ufficio provinciale di statistica (d.lgs. 6 settembre 1989, n. 322; codice in materia, Allegato A.3. al Codice) (*Nota* 20 giugno 2010).

Per quanto riguarda i trattamenti di dati effettuati a fini di ricerca storica, tra i casi più rilevanti si segnala un quesito posto da un comune in ordine alla possibilità di permettere ad un istituto di storia della resistenza di consultare i registri cimiteriali al fine di effettuare talune ricerche storiche. L'Amministrazione è stata al riguardo invitata a verificare,

nella comunicazione dei dati finalizzata alla ricerca storica, il rispetto della normativa di settore (cfr. art. 101 ss. del Codice; d.lgs. 29 ottobre 1999, n. 490, modificato dal d.lgs. 22 gennaio 2004, n. 42, richiamato dall'art. 103 del Codice, nonché il "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici*", Allegato A.2. al Codice, in *G.U.* 5 aprile 2001, n. 80) (*Nota* 25 ottobre 2010).

I medesimi princìpi sono stati richiamati con riferimento al testo di un accordo, sottoposto dal Ministero per i beni e le attività culturali, volto a consentire la riproduzione digitale dei registri di stato civile (napoleonico e postunitario) conservati presso gli Archivi di Stato, per la pubblicazione delle immagini e la indicizzazione dei dati ivi contenuti. È stato rappresentato al Ministero che qualunque soggetto pubblico può avvalersi, per lo svolgimento delle proprie funzioni istituzionali, del contributo di un soggetto privato designandolo "*responsabile del trattamento*" (art. 29 del Codice), qualora coadiuvi l'amministrazione trattando dati personali nell'ambito di un'attività che ricade nella sfera di titolarità della stessa amministrazione pubblica. È stato poi evidenziato che il titolare del trattamento è tenuto a rispettare le regole di correttezza e di non discriminazione nei confronti degli utenti, indipendentemente dalla loro nazionalità, categoria di appartenenza e livello di istruzione, individuate nel codice di deontologia e buona condotta cit. (art. 1, comma 3, lett. *a*)). Inoltre, in caso di rilevazione sistematica dei dati realizzata da un archivio in collaborazione con altri soggetti pubblici o privati, per costituire banche dati di intere serie archivistiche, la struttura interessata sottoscrive una apposita convenzione per concordare le modalità di fruizione e le forme di tutela dei soggetti interessati, attenendosi alle disposizioni della legge, in particolare per quanto riguarda il rapporto tra il titolare, il responsabile e gli incaricati del trattamento, nonché i rapporti con i soggetti esterni interessati ad accedere ai dati (art. 5, comma 4, del codice di deontologia cit.). Infine, è stato fatto presente al Ministero che le iniziative da adottare, anche nell'ambito di convenzioni, non devono essere sottoposte al vaglio di questa Autorità (*Nota* 11 gennaio 2011).

7. L'ATTIVITÀ DI POLIZIA

7.1. 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 e di uffici periferici della polizia di Stato a 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.

7.2. ALTRI INTERVENTI IN RELAZIONE AD ULTERIORI ATTIVITÀ DI FORZE DI POLIZIA

Nel riscontrare un quesito posto dal Dipartimento della pubblica sicurezza sulle modalità di acquisizione dei dati di georeferenziazione nell'espletamento dei compiti di polizia giudiziaria disciplinati dall'art. 55 c.p.p., con particolare riferimento ai dati relativi all'ubicazione di cui alla lett. *c*), dell'art. 1, del d.lgs. 30 maggio 2008, n. 109 (di attuazione della Direttiva n. 2006/24/CE, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione), l'Autorità ha chiarito che ove i dati prescindano da una comunicazione fra soggetti, e non siano quindi qualificabili come "dati di traffico" (si tratta dei dati reperibili, in tempo reale, nel *cd.* "*HLR-Home Location Register*" tenuto dai gestori telefonici, che non vengono conservati dal gestore se non temporaneamente, fino a spostamento dell'apparecchio in altra cella), non trova applicazione la particolare disciplina posta dagli artt. 123 e 132 del Codice. Al riguardo, l'Autorità ha richiamato il *provvedimento* concernente l'acquisibilità di tali informazioni relative a persone disperse da parte degli organismi di soccorso preposti a ricerche in montagna (*Provv.* 19 dicembre 2008 [doc. *web* n. 1580543]).

Al contrario, i dati relativi all'ubicazione delle apparecchiature di comunicazione mobile che presuppongono necessariamente una comunicazione fra soggetti devono essere considerati "dati di traffico", in quanto relativi alla cella da cui una chiamata di telefonia

mobile ha origine o nella quale si conclude. Tali dati sono conservati dai gestori nel rispetto delle disposizioni degli artt. 123 e 132 del Codice (quest'ultimo come modificato dal d.lgs. n. 109/2008); ai fini della loro acquisizione si applica quindi la disciplina dettata dal menzionato art. 132 che, al comma 3, ne prevede l'acquisibilità solo previa emanazione del decreto motivato del pubblico ministero.

7.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

Si è riferito nella *Relazione* 2009, p. 123, del *provvedimento* con cui il Garante, all'esito di accertamenti che si sono sviluppati nel corso del 2009, ha prescritto al Ministero dell'interno-Dipartimento della pubblica sicurezza di adottare alcune misure volte a rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen.

Il Dipartimento ha fornito riscontro nel termine assegnato, illustrando le iniziative intraprese al fine dare attuazione alle prescrizioni.

L'Autorità, nel prendere positivamente atto di tali iniziative, ritenute in linea con gli adempimenti richiesti, ha peraltro prescritto al Ministero dell'interno di indicare una precisa e definita tempistica di effettiva e concreta realizzazione delle misure prescritte.

Accesso diretto

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nell'N-SIS (sezione nazionale del Sistema informativo Schengen), 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, tuttavia, ancora pervengono direttamente al Garante non hanno subito sostanziali variazioni rispetto all'anno precedente (v. *Relazione* 2009, p. 124).

Anche nel 2010 sono aumentate le richieste di accesso ai dati pervenute al Garante da autorità di controllo di sezioni nazionali del SIS di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicate, previa consultazione degli Uffici segnalanti, nel rispetto delle disposizioni degli artt. 109 e 114 della Convenzione.

8. Attività giornalistiche

8.1. Minori

Il Garante si è occupato nuovamente del delicato tema del rapporto tra libertà di informazione e tutela della riservatezza dei minori.

Vittime di abusi

L'Autorità è intervenuta d'urgenza con un *provvedimento* di blocco temporaneo del trattamento nei confronti di alcuni quotidiani che, nel riferire dell'avvio di un'indagine a carico di un personaggio di rilievo pubblico su presunti abusi sessuali ai danni della nipote minorenne, avevano diffuso dati ritenuti idonei a identificarla indirettamente (*Provv.* 25 giugno 2010). In particolare i quotidiani avevano indicato il legame parentale che legava la minorenne con l'indagato, individuato nominativamente, unitamente ad altre informazioni relative alla famiglia, nonché divulgato alcuni dettagli del referto stilato dai medici a seguito degli accertamenti sanitari compiuti sulla bambina. L'Autorità ha rilevato che, anche quando la vittima non viene individuata nominativamente, la diffusione di altre dettagliate informazioni che la riguardano può comunque renderla riconoscibile, in particolare nella cerchia delle relazioni sociali degli interessati e ciò costituisce una violazione del codice di procedura penale (art. 114, comma 6, c.p.p.), del codice di deontologia per l'attività giornalistica (art. 7) e della Carta di Treviso. Tale valutazione è stata confermata anche dopo il completamento dell'istruttoria e pertanto l'Autorità ha disposto nei confronti dei quotidiani interessati il definitivo divieto di ogni ulteriore diffusione di qualunque informazione idonea, anche indirettamente, a identificare la minore e a fornire dettagli del referto medico (*Provv.* 8 luglio 2010).

Analogo *provvedimento* di divieto è stato adottato nei confronti di un'emittente televisiva in relazione a una trasmissione nella quale è stata ospitata una ragazza ventunenne che ha affermato di essere stata vittima, quando era bambina, di ripetuti episodi di violenza sessuale da parte di uno zio. Nel corso della trasmissione, in risposta a una specifica domanda della conduttrice, la ragazza ha dichiarato che anche la sorella più piccola –ora quattordicenne e adottata– è stata vittima di episodi analoghi, e ha fornito alcuni elementi idonei a identificare indirettamente la sorella, in particolare il proprio cognome e il luogo

di svolgimento dei fatti di violenza. L'Autorità ha rilevato una violazione delle disposizione a tutela dei minori sopra richiamate (art. 114, comma 6, c.p.p.; art. 7 del codice di deontologia giornalistica; Carta di Treviso) le quali –ha ribadito– operano a maggior ragione con riferimento a minori vittime di violenze di natura sessuale. La stessa Autorità ha poi ritenuto irrilevante la circostanza che sia stata l'ospite della trasmissione a diffondere le notizie relative alla sorella in quanto, a prescindere dalla facoltà dell'ospite intervistato di raccontare liberamente la propria storia, incombe sul conduttore-intervistatore e sulla società emittente l'onere di rispettare le disposizioni di legge sopra richiamate impedendo che vengano diffuse, anche nel corso di interviste rilasciate da altri soggetti, informazioni idonee a identificare i minori. Nel caso di specie, tra l'altro, era emerso che la diffusione delle informazioni relative alla bambina era avvenuta su sollecitazione della conduttrice (*Provv.* 16 settembre 2010 [doc. *web* n. 1753383]).

Figli di personaggi noti

La *ratio* delle disposizioni a tutela dei minori consiste nel prevenire e/o eventualmente vietare un'informazione idonea a lederne la personalità e a comprometterne un armonico sviluppo. Come indicato nella Carta di Treviso, tale eventualità può non configurarsi se la notizia inquadra il minore in un contesto positivo. Tale principio, già ricordato dal Garante (cfr. *Relazione* 2009, pp. 126 e 127), ha ispirato la risposta a una segnalazione riguardante un servizio giornalistico con immagini che documentavano in termini positivi la dimensione familiare e affettiva di un noto esponente politico, dimensione a cui lo stesso esponente ha sempre dato autonomo risalto (cfr. anche art. 6 comma 2, del codice di deontologia cit.) (*Nota* 8 ottobre 2010). Analoghi princìpi hanno ispirato la risposta a una segnalazione relativa a un servizio giornalistico avente ad oggetto il nuovo film di un noto regista italiano ispirato al tema dei rapporti familiari, servizio contenente immagini che rappresentano il contesto delle relazioni familiari e affettive di alcuni dei protagonisti del film e che ritraggono la figlia minore dei segnalanti in quanto parte anch'essa del *cast* (*Nota* 26 aprile 2010).

Controversie familiari

In relazione a diverse segnalazioni riguardanti la trattazione, da parte degli organi di informazione, di vicende familiari che hanno portato all'allontanamento di un minore dai genitori e il suo affidamento ai servizi sociali, l'Autorità è stata chiamata a cogliere il punto

di equilibrio tra diritto di cronaca e di critica su provvedimenti giurisdizionali in materia di famiglia e il rispetto della sfera privata del minore, interessato da detti provvedimenti.

Il Garante, nel rispondere alle segnalazioni ha rilevato che non si può escludere in assoluto che provvedimenti in materia di rapporti familiari possano essere oggetto di cronaca e critica giornalistica.

Ciò premesso, la valutazione deve essere sempre fatta caso per caso. In uno dei casi esaminati, infatti, durante una trasmissione televisiva sono state riferite informazioni delicate (necessità di assunzione di psicofarmaci, asserite molestie sessuali) riconducibili a una minore identificata non solo indirettamente mediante la rivelazione dell'identità del padre intervistato, ma anche direttamente, attraverso la divulgazione del nome della stessa riproposto ripetutamente attraverso una didascalia in continuo scorrimento sul video durante l'intervista del padre. In questo caso l'Autorità ha ritenuto detto trattamento, nel suo insieme, non idoneo a soddisfare l'obiettivo di salvaguardia dell'interesse del minore sopra richiamato e ne ha dato comunicazione all'emittente televisiva interessata (*Nota* 15 ottobre 2010).

Adozioni

Il trattamento delle informazioni riguardanti vicende adottive presenta aspetti delicati anche quando coinvolge soggetti non più minori, trattandosi di informazioni che ricevono di per sé una particolare protezione da parte dell'ordinamento (l. 4 maggio 1983, n. 184 "*Disciplina dell'adozione e dell'affidamento dei minori*", modificata dalla l. 28 marzo 2001, n. 149).

L'Autorità è intervenuta nei confronti di una trasmissione televisiva che ha dedicato ripetutamente uno spazio alla narrazione di storie di adozione. In particolare, sulla base di alcune segnalazioni pervenute, il Garante ha ravvisato la necessità di disporre d'urgenza il blocco del trattamento dei dati trattati nel corso di alcune puntate in quanto ritenute in contrasto con la disciplina in materia di protezione dei dati personali e con la legge sull'adozione sopra citata (*Provv.* 8 aprile 2010 [doc. *web* n. 1718160].

Nelle more dell'istruttoria è stata riscontrata la violazione del *provvedimento* di blocco essendo stati trattati nuovamente dati personali attinenti alla vicenda adottiva raccontata nel corso di una delle puntate oggetto del blocco; l'Autorità ha quindi contestato all'emittente

televisiva la sanzione amministrativa di cui all'art. 162, comma 2-*ter* del Codice nonché segnalato il caso all'autorità giudiziaria per eventuali valutazioni di competenza (art. 170).

Inoltre, esaurita l'istruttoria, l'Autorità ha ribadito la propria valutazione in ordine all'illiceità di alcuni trattamenti.

Il Garante ha infatti rilevato che erano stati trattati dati personali relativi a vicende adottive, nonché diffusi dati idonei a identificare le predette persone, spesso associati a delicate informazioni sul loro passato. L'Autorità ha inoltre rilevato che gli appelli lanciati e le scritte apparse in sovraimpressione nel corso della trasmissione avevano evidenziato come il trattamento dei dati avesse come scopo la ricerca degli adottati da parte di membri della famiglia naturale di origine; ciò, in contrasto con la *ratio* della disciplina sulle adozioni la quale individua specificamente quali sono i presupposti perché l'adottato possa accedere a informazioni che riguardano la sua origine e l'identità dei genitori biologici, delineando un percorso preordinato a tutelare, attraverso particolari procedure e l'intervento dei soggetti e delle istituzioni competenti, la personalità dell'adottato –anche divenuto maggiorenne– e i contesti familiari interessati (artt. 27, 28, e 73, l. 4 maggio 1983, n. 184, modificata dalla l. 28 marzo 2001, n. 149). Alla luce di tali valutazioni, il Garante ha vietato l'ulteriore trattamento dei dati relativi alle vicende esaminate e ha, in termini generali, raccomandato all'emittente interessata di assicurare la dovuta osservanza delle disposizioni in materia di adozione (*Provv.* 6 maggio 2010 [doc. *web* n. 1718239]). Il *provvedimento* è stato impugnato dall'emittente ed è pendente giudizio dinanzi al giudice civile.

8.2. CRONACHE GIUDIZIARIE

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

Pubblicazione di atti processuali

A seguito della diffusione su due siti Internet di un'ordinanza di custodia cautelare in carcere, pubblicata a corredo di una notizia concernente un presunto caso di corruzione, il destinatario della misura restrittiva si è rivolto al Garante lamentando un'illecita diffusione di dati "*di natura riservata e personale*", quali i numeri delle utenze cellulari oggetto di intercettazione, citati nel *provvedimento*. Compiuta l'istruttoria, il Garante ha accolto le richieste del segnalante, rilevando come la diffusione del *provvedimento* integrasse un trattamento a cui applicare la normativa *privacy* in materia di attività giornalistica.

Pertanto, pur riconoscendo il diritto alla manifestazione del pensiero da parte dell'associazione gestrice dei siti, che può esercitarsi anche mediante la pubblicazione di atti giudiziari non più coperti da segreto, il Garante ha ritenuto che la diffusione di dati quali i numeri di telefono, la residenza e i codici fiscali del segnalante e delle altre persone citate nel testo dell'ordinanza, avvenuta attraverso la pubblicazione in forma integrale del provvedimento giudiziario, abbia violato il principio dell'essenzialità dell'informazione, trattandosi di informazioni strettamente personali sicuramente sovrabbondanti e non indispensabili per rappresentare la vicenda giudiziaria.

Il Garante ha quindi vietato l'ulteriore diffusione disponendo la rimozione delle informazioni eccedenti dai due siti (*Provv.* 29 settembre 2010 [doc. *web* n. 1763096]).

Analoghe considerazioni sono state svolte in relazione alla pubblicazione delle utenze intercettate riportate nel documento inviato dalla Procura della Repubblica di Milano alla Giunta per le autorizzazioni a procedere della Camera dei deputati in relazione all'inchiesta che ha visto coinvolto, tra gli altri, il Presidente del Consiglio (*Nota* 20 gennaio 2011 e *Comunicato stampa* 21 gennaio 2011).

L'Autorità, anche in seguito a una segnalazione, ha avviato un'istruttoria in merito alla pubblicazione, anche su testate *online*, dell'audio degli interrogatori effettuati nell'ambito delle indagini sull'omicidio di una giovane donna di Avetrana. Tale circostanza è stata tempestivamente segnalata alla Procura della Repubblica che stava svolgendo le indagini la quale, come diffuso il 24 novembre 2010 dall'agenzia ANSA, ha provveduto al sequestro di detto materiale in relazione all'ipotesi di reato di "*pubblicazione arbitraria integrale di atti e documenti di un procedimento penale*".

Il richiamato parametro dell'essenzialità dell'informazione ha infine costituito la base nella valutazione di diversi trattamenti giornalistici che, pur se attinenti a fatti giudiziari di rilevante interesse pubblico, contenevano riferimenti a soggetti terzi i cui dati identificativi erano meritevoli di tutela –ad es., familiari, anche minorenni, di persone interessate da procedimenti penali (*Nota* 8 settembre 2010), parti lese (*Nota* 25 giugno 2010), ecc.– oppure a fatti pur relativi alle persone indagate ma estranei a quelli di indagine (ad es., il riferimento al ripetuto mancato superamento dell'esame d'avvocato da parte di un soggetto destinatario di un provvedimento di perquisizione (*Nota* 29 ottobre 2010).

Immagini di arresti

Il Garante è tornato ad occuparsi della pubblicazione delle fotografie che documentano operazioni di arresto e di quelle propriamente "segnaletiche".

Nel valutare alcune segnalazioni, il Garante ha ribadito il principio secondo il quale, di regola, è possibile pubblicare notizie relative a operazioni di arresto, salvo i limiti relativi alla diffusione di immagini che ritraggono persone in manette, di foto segnaletiche e di immagini comunque lesive della dignità della persona (art. 8 del codice di deontologia; cfr. anche *Relazione* 2007, par. 8.2.).

Ad avviso dell'Autorità, tali limiti sono stati superati in un caso nel quale è stata diffusa la foto segnaletica di una persona della quale sono stati oscurati solo gli occhi e di cui, sotto il riquadro della foto, sono state riportate le iniziali, rendendola di fatto riconoscibile. Uno dei quotidiani interessati dalla segnalazione aveva pubblicato anche le complete generalità della persona fotografata. Analoga valutazione è stata effettuata in un altro caso in cui, pur non essendovi elementi dai quali potesse desumersi, in base alle caratteristiche della foto, che si trattasse di una foto segnaletica, l'immagine pubblicata è apparsa lesiva della dignità della persona in quanto ritratta con la testa fasciata a seguito delle medicazioni ricevute. I predetti rilievi sono stati comunicati alle testate interessate, le quali si sono attivate per rimuovere le foto ancora presenti sulle edizioni *online* (*Note* 15 e 18 novembre 2010).

8.3. DATI SULLA SALUTE

Anche nel periodo di riferimento, come nel passato, si è reso necessario un richiamo al rispetto delle disposizioni che tutelano la riservatezza e la dignità di persone malate sia da

parte delle strutture sanitarie che forniscono informazioni sui loro pazienti sia da parte degli organi di informazione che accedono a tali informazioni (art. 83 del Codice; artt. 9, 10, 11 e 31 del codice di deontologia medica; art. 10 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; cfr. anche *Relazione* 2009, par. 8.4.).

Ciò è avvenuto per il caso di un giornale locale che aveva riferito sullo stato di salute di una persona ricoverata presso una struttura sanitaria, identificata con nome e cognome, descrivendo altresì la peculiare situazione in cui questa si era venuta a trovare (il fatto di essere stato "*dimenticato alla casa di riposo*" di cui "*nessuno pagava la retta*", le sue difficoltà di inserimento e di comunicazione all'interno della struttura, ecc.) (*Nota* 17 dicembre 2010).

Il Garante ha avuto altresì occasione di ricordare che la tutela della riservatezza e della dignità di una persona malata non viene meno neanche dopo il suo decesso (*Nota* 29 marzo 2010).

In seguito alla vicenda di un aborto farmacologico a Bari, il Garante ha invitato gli organi di informazione a tutelare l'anonimato e la riservatezza delle donne che effettuano interventi di interruzione della gravidanza (*Comunicato stampa* 8 aprile 2010).

8.4. ESPRESSIONE ARTISTICA E LETTERARIA

Nel periodo di riferimento diverse segnalazioni hanno prospettato una possibile illiceità del trattamento di dati personali, nell'ambito di pubblicazioni letterarie o comunque non giornalistiche in senso stretto (saggi, autobiografie, dizionari).

Nel fornire riscontro al riguardo, il Garante ha ricordato che l'art. 136, inserito nel Titolo XII della Parte II, del Codice ed intitolato "*Giornalismo ed espressione letteraria artistica*", estende l'applicazione delle disposizioni contenute nel Titolo stesso anche al trattamento "*temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale, di articoli, saggi e altre manifestazioni del pensiero*" (lett. *c*)) e che anche in relazione a tali trattamenti deve essere assicurato un bilanciamento tra la libertà di manifestare il proprio pensiero e il diritto alla riservatezza e alla protezione dei dati personali.

Pertanto –ha precisato il Garante– trovano applicazione le disposizioni che tutelano i minori e le informazioni sullo stato di salute; quelle che limitano la diffusione ai soli dati "*essenziali*" alla completezza dell'informazione e che danno rilievo alla particolare qualificazione dei personaggi citati nella narrazione (ad es., figure di rilevo pubblico) e, ancora, che consentono la pubblicazione delle informazioni già rese note dagli interessati (*Note* 11 giugno, 8 settembre, 14 dicembre 2010 e 5 gennaio 2011).

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

Nel 2010 sono pervenute segnalazioni e reclami relativi alla diffusione di dati personali concernenti personaggi pubblici o persone che esercitano pubbliche funzioni.

Il Garante ha ribadito il principio in base al quale vi sono margini più ampi nella diffusione di informazioni relative a tali persone, le quali possono riguardare, entro certi limiti, anche notizie attinenti alla vita privata.

L'Autorità tra l'altro, è intervenuto su un caso di diffusione di dati sanitari da parte di un quotidiano locale, che in un articolo aveva riportato, in fotografia, parte della cartella clinica del presidente di una regione e il referto di un altro esame sempre relativo al medesimo presidente.

Nel testo del *provvedimento*, si è rilevato che il servizio oggetto del reclamo riportava un fatto che può ragionevolmente considerarsi di rilievo pubblico, in quanto dava conto di una denuncia di presunta falsificazione della cartella clinica relativa al reclamante, presentata dal primario presso cui il reclamante aveva effettuato gli accertamenti clinici (denuncia che ha determinato l'apertura di un'indagine da parte della Procura della Repubblica).

In proposito, il Garante ha giudicato pertinente e non eccedente la diffusione della scheda di dimissione ospedaliera, ma non quella del referto, in quanto in quest'ultimo documento comparivano dettagli clinici ritenuti non essenziali. Il codice deontologico citato prevede, infatti, che "*la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita privata*" (art. 6) (*Provv.* 13 gennaio 2011 [doc. *web* n. 1787902]).

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

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

8.6. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

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

Giornali *online*

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

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

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

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

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

Informazioni *online*

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

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

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

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

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

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

9.1. Diffusione di dati sensibili su Internet

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

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

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

9.2. *Forum* e *blog*

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

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

Libera manifestazione del pensiero

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

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

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

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

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

Dati sanitari

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

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

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

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

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

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

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

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

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

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

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

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

9.3. *FACEBOOK*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Raccolta del consenso per diverse finalità e modalità del trattamento

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

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

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

Il Registro delle opposizioni

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

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

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

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

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

Modelli di informativa resa agli abbonati dagli operatori telefonici

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

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

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

eventualmente con quali dati (ad. es., solo con il cognome e l'iniziale del nome). Il secondo modello é relativo ai vecchi abbonati e dovrà essere inviato alla prima occasione utile di contatto (rendiconti, fatture, altre comunicazioni di servizio) oltre che essere inserito nei siti *web* degli operatori. Il modello dovrà specificare che l'abbonato ha sempre diritto di cancellarsi in ogni momento dagli elenchi telefonici.

Si evidenzia che il mancato rispetto delle prescrizioni del Garante comporterà sanzioni amministrative da un minimo di 30.000 ad un massimo di 180.000 euro, che potranno raggiungere, nei casi di violazione più grave, i 300.000 euro.

Obbligo di rendere l'informativa con riguardo alla raccolta dei dati presso terzi

Con riguardo all'obbligo di rendere l'informativa, quando i dati non sono raccolti presso l'interessato, all'atto della registrazione degli stessi o al più tardi, quando ne è prevista la comunicazione, non oltre la prima comunicazione (art. 13, comma 4, del Codice), l'Autorità ha ricevuto diverse istanze di esonero ai sensi dell'art. 13, comma 5, lett. *c*), del Codice e di conseguente individuazione di modalità equipollenti per informare gli interessati qualora l'informativa in forma individualizzata comporti un impiego di mezzi che il Garante dichiari manifestamente sproporzionato rispetto al diritto tutelato.

L'Autorità ha, in ragione delle diverse fattispecie esaminate, assunto differenti determinazioni. In alcuni casi ha respinto l'istanza di esonero, in particolare, con riguardo a dati estratti dal DBU (*database* telefonico unico), in ragione del fatto che i trattamenti che il titolare intendeva svolgere con l'ausilio di tali dati esulavano dalle finalità per le quali detto *database* è stato costituito. Il Garante ha infatti ribadito che il DBU rappresenta un archivio elettronico unico, contenente i dati personali dei clienti di tutti gli operatori di telefonia fissa e mobile per la formazione degli elenchi telefonici e la fornitura dei servizi di informazione abbonati, e pertanto non può essere utilizzato per finalità diverse da quelle per le quali è stato costituito se non in violazione dell'art. 11, comma 1, lett. *b*), del Codice (*Provv.* 16 settembre 2010 [doc. *web* n. 1753351]).

Con specifico riguardo all'offerta di servizi integrati di *mailing* postale per finalità di comunicazione commerciale e di *marketing*, è infatti emerso che diverse società, pur raccogliendo i dati presso terzi, non avevano fornito agli interessati l'informativa né al momento della registrazione, né al momento della prima comunicazione così come stabilito dal cit.

art. 13, comma 4 del Codice, essendo invalsa la prassi di rendere l'informativa con il primo *mailing* postale inviato per conto dei propri clienti o direttamente da questi ultimi. A fronte dei provvedimenti emanati dall'Autorità che hanno vietato il trattamento in assenza dell'informativa, prevista dall'art. 13, comma 4, del Codice, sono successivamente pervenute al Garante istanze di esonero ai sensi del successivo comma 5, lett. *b*), della norma. L'Autorità ha valutato la sussistenza dei presupposti per disporre l'esonero (la sproporzione dei mezzi, con riguardo sia all'elevato numero di interessati, operatori economici ed istituzionali, sia all'onerosità di tali mezzi) e previsto l'adozione di misure alternative per consentire di rilasciare agli interessati un'adeguata informativa generale, con modalità idonee e di facile accesso. Ciò sia nel caso in cui i dati personali siano stati acquisiti direttamente da fonti pubblicamente accessibili, sia nel caso in cui siano stati forniti da società specializzate. Il Garante ha anche previsto, nel caso di cessione dei dati, un'integrazione dell'informativa rilasciata con il primo contatto commerciale con alcune specifiche informazioni, proprio in ragione dell'informativa generale rilasciata precedentemente ai sensi dell'art. 13, comma 5, lett. *b*), del Codice (*Provv.* 16 dicembre 2010 [doc. *web* n. 1781973]).

9.7. USO DELLA TECNOLOGIA *RFID* NELLE TESSERE *SKI-PASS*

L'Autorità ha affrontato anche il complesso tema dell'uso dei dati personali attraverso la tecnologia *RFID* (*Radio Frequency Identification*), in particolare con riguardo all'utilizzo di tessere *ski-pass* per l'accesso agli impianti sciistici di un vasto comprensorio sciistico del Nord Italia.

L'intervento ha fatto seguito ad una serie di accertamenti ispettivi, svolti dal Nucleo speciale *privacy* della Guardia di finanza, presso i gestori degli impianti sciistici per verificare il rispetto della normativa sulla protezione dei dati personali, soprattutto con riguardo alle modalità e finalità della raccolta dei dati personali degli sciatori, al rispetto degli obblighi di informativa, nonché degli obblighi di notificazione e di eventuale acquisizione del consenso degli interessati.

In particolare, il problema della notificazione del trattamento è stato esaminato alla luce dall'art. 37, comma 1, lett. *a*), del Codice rispetto al trattamento di dati che indicano la

posizione geografica di persone mediante una rete di comunicazione elettronica, oltre che del *provvedimento* 9 marzo 2005 sulle *cd.* "*etichette intelligenti*" [doc. *web* n. 1109493].

Le società che gestiscono impianti di risalita utilizzano infatti la tecnologia *RFID*, integrata nei *badge* che gli sciatori usano per l'apertura automatica dei tornelli di accesso agli impianti di risalita, al fine di agevolarne i transiti.

In ragione del rilascio anche di tessere nominative è stata verificata la possibilità di individuare la posizione geografica dello *ski-pass* (*cd.* "*geolocalizzazione*") e di ricostruire il percorso effettuato dall'utente nell'ambito del comprensorio sciistico, circostanza che implica l'obbligo di notificazione del trattamento al Garante ai sensi del citato art. 37, comma 1, lett. *a*), del Codice.

All'esito di un esame approfondito, anche nei profili tecnici, è emerso che il ricorso alla tecnologia *RFID* da parte dei gestori degli impianti consente attualmente solo di registrare l'ingresso dello sciatore all'impianto di risalita e che i *chip RFID* vengono attivati esclusivamente al varco di accesso con un raggio di azione di pochi centimetri, senza possibilità di lettura a distanza e di conseguente localizzazione del soggetto. Il problema di una possibile ricostruzione del percorso sciistico effettuato dagli utenti e della sussistenza di un conseguente obbligo di notificazione al Garante è emerso anche con riguardo ad un ulteriore servizio, fornito da alcuni gestori, attraverso l'uso di una carta *RFID* ricaricabile che consente al titolare di visualizzare, attraverso una consultazione *online*, il numero degli impianti utilizzati, il dislivello e la stima dei chilometri di pista percorsi. Anche in tal caso l'Autorità ha accuratamente verificato che i dati raccolti ed utilizzati per fornire il servizio non consentano l'individuazione del percorso dello sciatore, appurando altresì che il servizio, nella sostanza, consente al titolare della carta un accesso diretto, tramite Internet, ai propri dati personali.

Un ulteriore aspetto, oggetto di analisi da parte del Garante, ha riguardato l'obbligo di fornire l'informativa in merito all'utilizzo della tecnologia *RFID*, così come disposto dal citato *provvedimento* 9 marzo 2005, il quale prevede espressamente, in linea con l'orientamento europeo tuttora vigente, che il titolare del trattamento, nel fornire agli interessati l'informativa di cui all'art. 13 del Codice, deve indicare, oltre alle finalità e

modalità del trattamento, anche la presenza di etichette *RFID*, senza che gli interessati si attivino a riguardo.

In proposito, occorre altresì dare evidenza alla presenza di lettori che attivano l'etichetta; l'informativa può essere fornita anche attraverso appositi avvisi agevolmente visionabili per formato e posizionamento, nei luoghi in cui le etichette *RFID* sono utilizzate, ed in tal senso hanno già provveduto diversi gestori di impianti sciistici.

In questo quadro, l'Autorità ha fornito chiarimenti ad una società, indicando anche le misure necessarie per proteggere la riservatezza dell'utente, relativamente al trattamento di dati personali attraverso il servizio "*Ski performance card*", che consente di visualizzare dati relativi alle prestazioni sportive dello sciatore, previo inserimento di un codice univocamente associato al *tag RFID* presente nel relativo *ski-pass* (*Note* 15 e 21 dicembre 2010).

9.8. TRATTAMENTO DEI DATI PERSONALI NEL SETTORE DELLE TELECOMUNICAZIONI

Attivazione di servizi telefonici non richiesti

Diverse segnalazioni di utenti, lamentavano, a fronte dell'attivazione di contratti di abbonamento a servizi di telefonia non richiesti, il rifiuto da parte dei gestori telefonici di fornire la registrazione della conversazione telefonica intercorsa con l'operatore nel corso della quale viene acquisito il consenso all'attivazione del servizio (*cd.* "*verbal ordering*"). Ribadendo il proprio precedente orientamento il Garante (cfr. *Provv.* 8 luglio 2009 [doc. *web* n. 1638561]) ha stabilito che il diritto di accesso ai dati personali dell'interessato, contenuti nella registrazione telefonica, esercitato ai sensi dell'art. 7 del Codice, implica il dovere del titolare di mettere a disposizione copia della stessa al fine di consentire l'acquisizione del dato vocale in essa contenuto (*Note* 24 giugno e 7 luglio 2010).

Invio di comunicazioni commerciali non sollecitate (*spam*)

Anche nel 2010 il Garante ha ricevuto numerose richieste d'intervento relative ad attività di *spam* realizzata mediante diversi mezzi (posta elettronica, fax, chiamate telefoniche, *Sms*).

Rispetto all'anno precedente appaiono in leggera diminuzione le segnalazioni riguardanti la ricezione di fax indesiderati (soprattutto a partire dalla seconda metà dell'anno), anche in ragione degli interventi prescrittivi e sanzionatori effettuati nei confronti degli operatori telefonici (che risultavano essere i maggiori committenti di tale forma di promozione).

Il fax e l'e-mail restano comunque i mezzi più utilizzati per le attività di *spam* anche se, nel corso del 2010, si è notato un leggero incremento delle segnalazioni riguardanti la ricezione di *Sms* e telefonate pre-registrate, che può essere in parte collegato alle campagne elettorali svolte nel corso dell'anno.

Per quanto riguarda il contrasto allo *spam*, molti segnalanti hanno osservato una sensibile diminuzione dei contatti indesiderati a seguito dell'intervento del Garante; persistono, dall'altro lato, le violazioni soprattutto via e-mail, che rendono a volte difficile individuare il titolare del trattamento, per le modalità con cui si può operare in rete e perché spesso i titolari risultano avere sede in Paesi extraeuropei.

L'intervento dell'Autorità nel corso dell'anno è stato più incisivo soprattutto per quanto riguarda i provvedimenti emessi –pressoché raddoppiati rispetto all'anno precedente– e volti prevalentemente a contrastare il fenomeno dello *spam* via e-mail e, in misura maggiore, via fax.

In più occasioni, è stato vietato l'invio, mediante posta elettronica, di comunicazioni promozionali a terzi in assenza di informativa e consenso preventivo e specifico degli interessati ai sensi degli artt. 13 e 130 del Codice (*Provv.* 26 marzo 2010 [doc. *web* n. 1727662]; *Provv.* 8 aprile 2010 [doc. *web* n. 1721205]; *Provv.* 23 settembre 2010 [doc. *web* n. 1758527]).

Il Garante si è occupato anche del diffuso fenomeno dell'invio di fax pubblicitari a destinatari che non avevano mai ricevuto l'informativa né prestato il consenso, intervenendo con diversi provvedimenti inibitori e prescrittivi, accompagnati dall'emanazione delle conseguenti sanzioni amministrative (v. *provvedimenti* 26 marzo 2010 [doc. *web* nn. 1719901 e 1719891]; *Provv.* 6 maggio 2010 [doc. *web* n. 1729175]; *Provv.* 13 maggio 2010 [doc. *web* n. 1737799]; *Provv.* 3 giugno 2010 [doc. *web* n. 1738039]; *provvedimenti* 1 luglio 2010 [doc. *web* nn. 1737773 e 1738592]; *Provv.* 10 novembre 2010 [doc. *web* n. 1769487]; *Provv.* 26 gennaio 2011 [doc. *web* n. 1790365]; *Provv.* 3 febbraio 2011 [doc. *web* n. 1792588]).

In alcuni degli interventi, il Garante ha ricordato che quest'obbligo non può essere eluso inviando un primo messaggio che, nel richiedere il consenso, abbia già un contenuto promozionale (v. *Provv.* 29 maggio 2003, relativo allo *spamming* [doc. *web* n. 29840]).

Nell'occasione, è stato inoltre ribadito che la reperibilità dei dati sugli elenchi pubblici quali, ad esempio gli elenchi categorici, e il trattamento per lo svolgimento di attività economiche non consentono l'esonero previsto dall'art. 24, comma 1, lett. *d*), del Codice, e quindi non esimono il titolare del trattamento, in ragione della specificità del mezzo considerato, dal chiedere il consenso all'interessato per l'uso promozionale del telefax in considerazione della specifica disciplina prevista all'art. 130 del Codice.

Sempre in materia di *spam*, il Garante ha adottato diversi provvedimenti inibitori e prescrittivi anche nei confronti di società che, presumendo di poter inviare comunicazioni pubblicitarie in ragione dell'acquisto da terzi di *database*, non sono state in grado di fornire la documentazione attestante la manifestazione del consenso dei segnalanti al trattamento dei dati personali per finalità di ricezione di messaggi promozionali; in particolare è stato ribadito che, come previsto dal *provvedimento* 29 maggio 2003, relativo allo *spamming* cit., l'utilizzo di dati presenti in banche dati acquistate da terzi, nel caso di invio di comunicazioni automatizzate, deve essere preceduto da apposite verifiche da parte di chi acquista la banca dati stessa, per accertare l'espressione di consensi specifici ed informati degli interessati.

Più in generale, per l'attività di inoltro tramite sistemi automatizzati di messaggi promozionali in modo non sistematico, l'Autorità ha inviato apposite note di richiamo al pieno rispetto della disciplina in materia.

Spam proveniente dall'estero

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: in diversi Paesi infatti la disciplina sulla protezione dei dati personali non garantisce le persone giuridiche.

Si è al riguardo richiesto l'inserimento del Garante nel sistema *CPC* (*Consumer Protection and Cooperation*) istituito dal Regolamento (CE) 2006/2004 e messo a punto dalla Commissione europea per consentire alle autorità competenti in materia di tutela dei consumatori dei Paesi membri di collaborare nelle investigazioni che riguardano illeciti commessi in ambito transfrontaliero fornendo, allo stesso tempo, un *database* condiviso per lo scambio di informazioni su una piattaforma sicura.

9.9. "NUOVE FRONTIERE" DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: APPROFONDIMENTO SULL'UTILIZZO DELLE *APPLICATION* PER *SMARTPHONE* E *TABLET*

È stata avviata una complessa istruttoria in materia di *software* di vario tipo (giochi, musica, guide di natura diversa, *social network*, ecc.) che possono essere "scaricati" ed installati su *smartphone* e *tablet* per fornire a tali dispositivi alcune funzionalità aggiuntive (ad es., per la gestione del portfolio clienti o del calendario aziendale, per la condivisione di foto, video ed informazioni, per il monitoraggio dei propri movimenti bancari, per memorizzare ed elaborare testi o immagini, per localizzare ed essere localizzati da altri utenti, per redigere programmi in base alle proprie abitudini di consumo, per archiviare informazioni sulla salute).

L'Autorità ha richiesto informazioni ad alcuni produttori di sistemi operativi per *smartphone* e *tablet*, *leader* a livello mondiale nel settore.

Ne è emerso, anche esaminando alcune segnalazioni pervenute, che gli utenti che si avvalgono di tali applicazioni non sempre sono consapevoli dei rischi relativi al trattamento dei propri dati personali, soprattutto in ordine ai destinatari di tali dati, ai loro possibili utilizzi, al tempo di conservazione delle informazioni, alla loro archiviazione non sul dispositivo dell'utente, ma sulla *cloud* di un fornitore del servizio in modalità *web*, ecc.

L'Autorità sta esaminando i meccanismi volti ad informare gli utenti delle possibili modalità e finalità del trattamento dei dati personali e dei connessi rischi, quali *policy* interne, misure di sicurezza e ulteriori misure e attività di correzione ed *enforcement*, eventualmente previste per le ipotesi di violazione delle dette *policy* o di trattamenti illeciti dei dati personali.

Ciò, al fine di verificare la loro compatibilità con regole e princìpi *standard* in materia di protezione dei dati personali (quali i princìpi di proporzionalità e necessità), come emergenti anche da alcuni documenti elaborati dal Gruppo Art. 29 (cfr., *ex multis*: WP 163 del 12 giugno 2009 sui *social network online*; WP 171 del 22 giugno 2010 sulla pubblicità comportamentale).

10. PROPAGANDA ELETTORALE E ASSOCIAZIONI

L'Autorità si è occupata di una vicenda avente ad oggetto il trattamento di dati personali da parte di un'associazione a carattere notoriamente politico.

Con due distinte segnalazioni, era stata infatti contestata un'indebita divulgazione di dati personali sensibili relativi ad alcune aderenti, conseguente all'affissione nella bacheca (sita lungo il corso principale del paese) di un comunicato concernente l'espulsione delle segnalanti dall'associazione.

Questa aveva replicato che le istanti –la cui militanza politica era già nota presso la compagine locale, anche a seguito della loro partecipazione a precedenti appuntamenti elettorali– avevano appoggiato, nel corso di una pregressa campagna elettorale, una lista antagonista a quella ufficialmente sostenuta dal partito cui le stesse aderivano. L'affissione, pertanto, aveva risposto principalmente all'esigenza necessità di informare correttamente l'elettorato, disorientato dal comportamento delle segnalanti.

Al riguardo, il Garante ha ritenuto che l'affissione, considerato anche il contesto circoscritto e il momento in cui era avvenuta, risultava essere stata effettuata nel perseguimento di un legittimo interesse alla trasparenza e alla corretta informazione degli appartenenti alla compagine locale, sicché il correlato trattamento non poteva considerarsi illecito in relazione a tale profilo; essa costituiva inoltre una manifestazione del pensiero, prevista e disciplinata, sotto il profilo della protezione dei dati personali, dall'art. 136 ss. del Codice né, nel caso di specie, risultavano violati i limiti del diritto di cronaca avuto riguardo, in particolare, all'essenzialità dell'informazione.

Nondimeno, l'Autorità ha ritenuto sproporzionato il trattamento in relazione alla prolungata pubblicazione del comunicato (oggetto di affissione per alcuni mesi), essendo ormai venute meno, tenuto anche conto del ristretto contesto locale, le esigenze di trasparenza e chiarificazione prospettate dall'associazione. L'ulteriore diffusione è stata pertanto vietata (*Provv.* 23 dicembre 2010 [doc. *web* n. 1784951]).

Trattamento di dati sensibili da parte di un ente religioso

Sono pervenuti all'Autorità reclami e segnalazioni su possibili violazioni della disciplina in materia di protezione dei dati personali da parte di un ente religioso e di un'as-

sociazione di studi e ricerche nel campo della religiosità (di seguito "centro studi"), che in occasione dello svolgimento di una ricerca di tipo sociologico, avrebbero chiesto agli aderenti all'ente di compilare un questionario volto ad acquisire approfondite informazioni, anche di natura sensibile e, talora, riferite a terzi, su molteplici profili della loro vita personale (in specie, opinioni ed orientamenti politici; abitudini e tendenze sessuali; comportamenti in campo religioso; condizioni di salute; stili e scelte di vita su tematiche particolarmente delicate, quali l'interruzione della gravidanza).

A detta degli istanti il questionario, pur non contenendo i nominativi degli interessati, avrebbe comunque consentito di identificare i singoli compilatori, in virtù del possibile collegamento tra talune informazioni ivi contenute (quali l'anno di nascita, la città di residenza, la composizione del nucleo familiare, il ruolo rivestito nell'ambito dell'ente) ed altri dati sugli associati, detenuti dall'ente per altre finalità.

Le risultanze istruttorie non hanno consentito di ritenere provato l'avvenuto trattamento di dati personali di coloro che avevano aderito all'iniziativa (o di eventuali terzi), atteso che, stando alle dichiarazioni dell'ente e del centro studi, le informazioni fornite, per loro natura tali da non consentire l'identificazione "diretta" del compilatore o di terzi, non sarebbero state utilizzate, allo stato, dai soggetti coinvolti nell'attività di ricerca, neanche per l'identificazione "indiretta" degli interessati (cfr. art. 4, comma 1, lett. *b*) e *c*), del Codice); i soggetti contrari all'iniziativa, inoltre, non avevano compilato i questionari, sicché i loro dati personali non potevano essere stati trattati.

Tale ultima circostanza, confermata anche da ulteriori risultanze istruttorie, ha fatto venir meno ogni esigenza cautelare e, di conseguenza, ha reso non necessario l'esame delle richieste di blocco e di divieto del trattamento dei dati riferiti a taluni istanti.

Tuttavia, l'Autorità ha rilevato l'esistenza, presso l'ente, di un archivio nominativo e di altre fonti di informazione contenenti dati identificativi riferiti ai propri adepti, nonché di risorse tecnologiche presso il centro studi e la società esterna della quale il centro si era avvalso per l'analisi e l'elaborazione delle informazioni contenute nei questionari compilati, astrattamente in grado di permettere l'identificazione indiretta degli interessati, mediante un'interconnessione tra le informazioni riportate nei questionari –che, all'esito

dell'istruttoria curata dall'Autorità, erano ancora in possesso della menzionata società– e quelle conservate nel predetto archivio.

Analogamente, si è ritenuto che l'identificabilità indiretta degli interessati ai sensi del "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*" (Allegato A.4. al Codice) fosse agevolata, nel caso di specie, anche dal ristretto numero di membri dell'ente che avevano aderito all'iniziativa.

Pertanto, benché fossero stati adottati, in concreto, alcuni accorgimenti volti ad assicurare l'"anonimato" degli interessati, si è fatto presente che, soprattutto in considerazione della peculiare natura delle informazioni raccolte, tali accorgimenti avrebbero dovuto essere integrati con misure idonee ad impedire, fin dalla raccolta dei questionari compilati, anche l'indiretta identificabilità dei soggetti interessati alla rilevazione.

Il Garante ha pertanto prescritto al centro studi (in qualità di titolare della ricerca) di adottare accorgimenti idonei ad escludere il rischio di interconnessione tra i dati personali (in specie i nominativi) degli aderenti all'attività di ricerca (in possesso del solo ente religioso) e le informazioni contenute nei questionari, per evitare l'identificazione, sia pure in forma "indiretta", degli interessati.

A tal fine è stato prescritto di conservare i questionari in luoghi protetti da eventuali accessi indebiti, di non trasmetterli ad alcuno dei soggetti coinvolti nel progetto e di distruggerli al termine della ricerca. Al medesimo scopo, è stato disposto, nei confronti dell'ente, il divieto di comunicare agli altri soggetti coinvolti nel progetto di ricerca e per le finalità ad essa connesse, i dati personali riferiti ai propri adepti dei quali era in possesso, in qualità di autonomo titolare, per finalità di tipo associativo (art. 154, comma 1, lett. *d*), del Codice).

Infine, è stato prescritto al centro studi, in occasione di future iniziative di studio dalle quali possa discendere un'identificazione, sia pure in forma indiretta, dei soggetti coinvolti, di assicurare la scrupolosa osservanza e la concreta attuazione delle disposizioni contenute nel "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*", il cui rispetto costituisce condizione di liceità e correttezza del trattamento dei dati personali effettuato dai soggetti ai quali dette disposizioni si

riferiscono (artt. 12, comma 3 e 11, comma 1, lett. *a*), del Codice) (*Provv.* 1° aprile 2010 [doc. *web* n. 1721183]).

In un altro caso, un istituto che opera nel settore della ricerca sulla storia contemporanea aveva chiesto all'Autorità chiarimenti in ordine alla conformità al Codice della pubblicazione di taluni documenti, inerenti una rilevante vicenda storica (in specie, la sentenza di proscioglimento di uno degli imputati nel procedimento penale che ne è derivato, prima del dibattimento per estinzione del reato dovuta ad amnistia).

L'Autorità ha richiamato l'attenzione dell'istituto sulla necessità di conformare puntualmente il trattamento dei dati personali in esame sia all'art. 52, comma 7 e alle disposizioni contenute nella Parte II, Titolo VII, del Codice, sia alle prescrizioni contenute nel codice di deontologia e di buona condotta adottato in materia (*Provv.* 14 marzo 2001 [doc. *web* n. 1556419]), con particolare riferimento a quanto disposto dal Capo III contenente "*regole di condotta per gli utenti e condizioni per la liceità dei relativi trattamenti*".

Tenuto conto della peculiare natura dei dati oggetto di trattamento, si è fatto altresì presente che lo stesso era stato già autorizzato dal Garante nei termini previsti dal capo V dell'autorizzazione n. 7 del 16 dicembre 2009, relativa al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici (*Nota* 12 gennaio 2010).

11. Le attività economiche e i rapporti di lavoro

11.1. Settore bancario

Nel periodo di riferimento l'attività in questo settore è stata principalmente rivolta alla trattazione dei casi prospettati a diverso titolo all'Autorità.

In uno di essi, in particolare, un reclamante aveva fatto presente che la moglie, dovendo svolgere normali operazioni *online* su un conto corrente cointestato con lo stesso reclamante, aveva utilizzato le credenziali a suo tempo attribuitele dalla banca per accedere ai servizi in rete. Benché le credenziali fossero pertinenti al solo conto cointestato, la digitazione aveva consentito di accedere ad un altro conto corrente di cui soltanto il reclamante era titolare ed intestatario, sicché il coniuge aveva avuto la possibilità di conoscere le movimentazioni bancarie su di esso effettuate ed il relativo saldo. Di conseguenza l'interessato aveva chiesto al Garante, previa adozione di un *provvedimento* di blocco dei dati trattati, di prescrivere alla banca le misure necessarie per rendere il suddetto trattamento conforme a legge.

Le risultanze istruttorie hanno consentito di accertare una indebita comunicazione a terzi (nel caso di specie, al coniuge del reclamante) di dati bancari, per omessa osservanza, da parte degli incaricati della banca, delle istruzioni loro impartite.

Pertanto, pur avendo verificato che la banca aveva adottato le misure "minime" di sicurezza a protezione dei dati dei clienti (artt. 33 e 34 del Codice; regole 1-26 dell'Allegato B.), il Garante ha prescritto di rafforzare le misure di sicurezza "idonee" di cui all'art. 31 del Codice, in modo da garantire la scrupolosa vigilanza sull'operato degli incaricati, sensibilizzarli al rispetto delle istruzioni ricevute in occasione di specifiche iniziative di formazione del personale e ridurre al minimo il rischio di errori operativi (*Provv.* 11 febbraio 2010 [doc. *web* n.1705119]).

In un altro caso, il reclamante aveva rappresentato che il proprio coniuge, nell'atto introduttivo del procedimento di separazione personale, aveva fatto riferimento ad informazioni che lo riguardavano, relative a rapporti contrattuali con la banca, producendo anche specifici documenti bancari. L'interessato si era quindi rivolto al Garante affinché fosse accertata l'illiceità della comunicazione a terzi dei suoi dati personali.

Dalle risultanze istruttorie è emerso che presso la banca era stato effettuato, in assenza di legittimo presupposto, un accesso ai dati bancari riferiti al reclamante. Ciò verosimilmente per il comportamento dell'incaricato della banca, che, senza fornire giustificazione, aveva consultato la posizione del reclamante, in un orario in cui l'interessato, unico soggetto deputato a ricevere tali informazioni, risultava inequivocabilmente in servizio presso la propria sede di lavoro (cfr. artt. 4, comma 1, lett. *h*), 30, 167 del Codice).

Anche in questo caso, il Garante, ha prescritto di rafforzare le misure di sicurezza "idonee" di cui all'art. 31 del Codice (*Provv.* 18 marzo 2010 [doc. *web* n. 1715015]).

In un ulteriore caso, l'interessato aveva segnalato che un importante gruppo bancario aveva contattato telefonicamente sua moglie, titolare di un mutuo chirografario appoggiato per il versamento delle rate su un conto corrente intestato in via esclusiva allo stesso segnalante ed acceso presso una banca del gruppo, per sollecitare il pagamento di una mensilità ancora non corrisposta. In tale occasione, tuttavia, la dipendente preposta avrebbe reso noto al coniuge dell'interessato anche ulteriori vicende concernenti lo stato del conto corrente (cioè l'esistenza di un fido concesso al titolare del rapporto e l'avvenuto sconfinamento rispetto al fido). Ritenendo tale comportamento contrario alla disciplina di protezione dei dati personali, l'interessato aveva chiesto al Garante l'adozione di misure atte ad impedire il ripetersi di episodi analoghi.

Al riguardo, in base ai princìpi in materia di trattamento di dati personali nell'esercizio dell'attività di recupero crediti (v. *Provv.* 30 novembre 2005 [doc. *web* n. 1213644]), il Garante ha ritenuto pertinente e non eccedente rispetto alla finalità di recupero crediti la comunicazione al mutuatario del numero di conto corrente, del nominativo del relativo intestatario, della banca di appoggio e dell'esito negativo del tentativo di addebito del conto per incapienza del medesimo, sempre che al titolare del rapporto di conto corrente fosse stata resa un'adeguata informativa. Ha, però, considerato sproporzionato il trattamento di informazioni concernenti l'esistenza di "fidi" o eventuali loro "sconfinamenti" del tutto ininfluenti ai fini di una corretta informazione del mutuatario sulle vicende strettamente inerenti al saldo dei ratei in scadenza. Nel caso in questione, tuttavia, le risultanze istruttorie non hanno consentito di ritenere comprovata la lamentata comunicazione anche di informazioni strettamente riguardanti il conto corrente del segnalante.

Dal momento che le misure "minime" di sicurezza poste a presidio dei dati trattati nell'esercizio delle attività di recupero crediti (artt. 33-35 del Codice e Allegato B. al Codice) erano state adottate, il Garante ha prescritto alla banca e alla società finanziaria di richiamare il responsabile e gli incaricati del trattamento al rispetto delle istruzioni già impartite.

L'Autorità ha altresì prescritto alla società finanziaria di comunicare al mutuatario solo i dati bancari pertinenti rispetto alle finalità di informare il titolare del finanziamento sulle vicende relative al mutuo e di consentirgli di regolarizzare la posizione debitoria; inoltre, al fine di verificare la tipologia e la pertinenza delle informazioni rese al debitore in caso di contestazioni, ha suggerito di privilegiare l'invio dei solleciti di pagamento mediante l'impiego di idonee modalità, quali, per esempio, la comunicazione elettronica all'indirizzo e-mail fornito dal debitore o, in difetto, la spedizione in plico chiuso presso il suo domicilio (*Provv.* 21 ottobre 2010 [doc. *web* n. 1771017]).

Un comune aveva lamentato la comunicazione da parte di una banca agli studi legali che assistevano alcuni creditori in procedimenti esecutivi presso terzi (nel caso di specie, la banca stessa) promossi nei confronti del Comune, gli estremi identificativi ed il nominativo delle parti di altri procedimenti esecutivi promossi nei confronti del comune medesimo. Ciò mediante l'invio di una sola missiva all'indirizzo di tutti i creditori procedenti.

Tale comunicazione, originata da procedimenti pendenti avanti al giudice civile, era eccedente ai sensi dell'art. 11, comma 1, lett. *d*), del Codice, rispetto alla finalità perseguita (consistente nell'informare i creditori procedenti circa le modalità con le quali la banca, in qualità di terzo, aveva provveduto ad adempiere agli obblighi imposti al custode dall'art. 547 c.p.c.), anche in considerazione del fatto che ciascun destinatario della comunicazione, ancorché creditore procedente in un distinto procedimento esecutivo, era terzo rispetto agli altri procedimenti. Poiché il comune non aveva prestato il consenso alla comunicazione (art. 23 del Codice) né ricorrevano i presupposti alternativi di cui all'art. 24 del Codice, la comunicazione stessa è stata ritenuta in violazione degli artt. 11, comma 1, lett. *d*) e 23 del Codice. Il Garante ha riservato ad un autonomo procedimento le valutazioni relative all'eventuale applicazione di sanzioni amministrative.

11.2. TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLA CENTRALE DEI RISCHI GESTITA DALLA BANCA D'ITALIA E DEI SISTEMI DI INFORMAZIONE CREDITIZIA (SIC)

Anche nel corso del 2010 sono pervenute all'Autorità segnalazioni e reclami riguardanti il trattamento dei dati personali posto in essere da banche dati pubbliche e private (Sistemi di informazione creditizia-SIC e Centrale dei rischi gestita dalla Banca d'Italia) e dalle banche e finanziarie che agiscono in qualità di partecipanti a tali sistemi.

Le segnalazioni hanno riguardato soprattutto l'informativa da fornire agli interessati, nonché il rispetto delle norme di condotta previste dal "*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*" (*Provv.* 16 novembre 2004 [doc. *web* n. 1556693] Allegato A.5. al Codice), che costituiscono condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali effettuati dai gestori e dagli utenti dei sistemi di informazioni creditizie (SIC).

Al riguardo, il Garante ha ribadito che i dati conservati nei SIC devono essere sempre corretti ed aggiornati e che l'iscrizione di una posizione debitoria in tali banche dati è lecita solo se ne è stato dato preavviso all'interessato.

Più in dettaglio, in un caso l'interessato aveva segnalato di essere venuto a conoscenza, in occasione di una richiesta di mutuo, dell'esistenza di una segnalazione negativa a suo nome presso un SIC, effettuata da parte di una finanziaria dalla quale aveva in passato ricevuto un prestito. Le risultanze istruttorie hanno consentito di accertare che il segnalante aveva pagato tutte le rate previste, ma che, presumibilmente per errore, una di tali rate non era stata registrata dalla società finanziaria. Quest'ultima, inoltre, prima di procedere all'iscrizione del nominativo dell'interessato nel SIC, non aveva provveduto ad inviargli l'avviso dell'imminente registrazione del suo nominativo nei SIC, come previsto dall'art. 4, comma 7, del suddetto codice di deontologia e di buona condotta. In considerazione di quanto sopra esposto, il Garante ha prescritto alla società finanziaria di disporre la cancellazione dal SIC dei dati riferiti al finanziamento sottoscritto dall'interessato (*Provv.* 16 settembre 2010 [doc. *web* n. 1753816]).

In un'altra segnalazione, relativa ad una complessa vicenda, una società ha rappresentato

di avere riscontrato la presenza del proprio nominativo in un sistema di informazioni creditizie, quale richiedente un prestito finalizzato. La segnalazione al SIC era stata effettuata da una finanziaria, alla quale la segnalante asseriva di non aver chiesto alcun finanziamento. Nel riscontro fornito all'Autorità, la società finanziaria rappresentava di aver ricevuto i dati da un'altra società, per valutare la richiesta di concessione di un fido per l'acquisto di beni formulata dalla segnalante a quest'ultima società. La comunicazione di dati e l'avvio dell'istruttoria nella richiesta di finanziamento erano, tuttavia, avvenute senza la previa informativa richiesta dall'art. 13 del Codice.

Il trattamento è risultato, pertanto, in contrasto con la previsione dell'art. 13 del Codice e non conforme alle regole di comportamento previste dal citato codice di deontologia.

Il Garante ha pertanto prescritto alle società titolari del trattamento rispettivamente di formulare un'informativa in stretta aderenza a quanto previsto dall'art. 13 del Codice e di osservare scrupolosamente e dare concreta attuazione alle regole di comportamento stabilite dal codice di settore (*Provv.* 6 maggio 2010 [doc. *web* n. 1737818]).

In un altro caso un segnalante, al quale era stato rifiutato un finanziamento, aveva appreso che presso un SIC risultava, a suo nome, un'operazione di "prestito rinunciato", a suo dire non corrispondente al vero.

Dall'istruttoria è emerso che tale dato non era esatto, non era stata fornita all'interessato l'informativa, ed il riscontro alle richieste avanzate dall'interessato stesso ai sensi dell'art. 7 del Codice era stato tardivo.

Pertanto il Garante ha prescritto alla banca di garantire il rispetto delle regole di comportamento stabilite dal codice di settore e di sensibilizzare in tal senso gli incaricati del trattamento, ribadendo l'essenzialità del rispetto di tale regole, nonché di assicurare che sia fornito un idoneo e tempestivo riscontro nei termini di legge a tutte le istanze ritualmente proposte ai sensi dell'art. 7 del Codice (*Provv.* 11 marzo 2010 [doc. *web* n. 1715024]).

L'Autorità ha poi dato corso a una segnalazione inviata dal presidente del consiglio di amministrazione di due società, il quale ha rappresentato di essere venuto a conoscenza della presenza di segnalazioni a carico delle società stesse presso il *cd.* "*servizio di prima informazione*" presso la Centrale dei rischi della Banca d'Italia, riguardanti richieste di

finanziamento. Tali segnalazioni sarebbero state "*abusive in quanto non corrispondenti ad alcuna richiesta di concessione di fido da parte delle due società*".

Dai riscontri forniti dalle menzionate società è emerso che, in un caso, la finanziaria aveva ricevuto una richiesta per una operazione di *leasing* da una persona incaricata dalla stessa società segnalante, alla quale, secondo quanto dichiarato dalla finanziaria era stata fornita in forma orale la necessaria informativa. Nell'altro caso invece, è risultato che la finanziaria aveva ricevuto i dati da un'altra società e non era stata data l'informativa ai sensi dell'art. 13 del Codice in merito alla comunicazione dei dati a terzi. All'esito dell'attività istruttoria il Garante, come in precedenti pronunce, ha confermato che la comunicazione dei dati alla Centrale dei rischi di Banca d'Italia, in quanto prevista da una normativa, non richiede il rilascio del consenso da parte degli interessati (art. 24, comma 1, lett. *a*), del Codice). Ha poi precisato che l'informativa deve essere fornita quando i dati sono raccolti direttamente presso gli interessati indicando anche "*i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati*", e che il titolare del trattamento non è tenuto a fornire la predetta informativa ove essi siano raccolti presso terzi e "*trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria*" (art. 13, comma 5, lett. *a*), del Codice).

Il Garante ha pertanto prescritto alla società che ha raccolto i dati dall'interessato e comunicato gli stessi alla finanziaria, di predisporre un'informativa in stretta aderenza a quanto previsto dall'art. 13 del Codice, nella quale sia riportata anche l'indicazione dei soggetti terzi ai quali i dati dei clienti potranno essere comunicati, riservando ad un autonomo procedimento le valutazioni di competenza in ordine all'eventuale applicazioni di sanzioni amministrative (*Provv.* 10 novembre 2010 [doc. *web* n. 1769502]).

11.3. SETTORE ASSICURATIVO

In ambito assicurativo, si menziona una segnalazione avente ad oggetto il trattamento di dati personali effettuato per il servizio di fornitura telefonica di preventivi.

L'istante aveva lamentato che l'operatrice del *call center* cui si era rivolto per ricevere un preventivo in ordine a una polizza assicurativa concernente la responsabilità civile

derivante dalla circolazione di veicoli a motore non aveva provveduto, successivamente al rilascio del preventivo, a cancellare i suoi dati personali forniti in occasione del contatto telefonico.

Il Garante ha ritenuto lecita, anche ai fini di una eventuale tutela degli operatori telefonici, l'acquisizione dei dati identificativi dell'interlocutore, utili altresì a consentire una reale "personalizzazione" del preventivo; ciò, tra l'altro, in osservanza di specifiche disposizioni legislative (art. 131 del d.lgs. 7 settembre 2005, n. 209) e regolamentari (artt. 5 e 7, regolamento ISVAP 9 maggio 2008, n. 23). È risultata inoltre giustificata l'acquisizione dei recapiti degli utenti nella misura in cui gli interessati abbiano espressamente manifestato la propria volontà di ricevere il preventivo per iscritto.

Per contro, l'Autorità ha ritenuto sproporzionata (art. 11, comma 1, lett. *d*), del Codice) l'acquisizione di altri dati da parte della compagnia, non essendone stata provata l'effettiva necessità e non eccedenza in relazione alla finalità concretamente perseguita; ciò, tenuto anche conto che la medesima compagnia avrebbe potuto, in astratto, ricorrere a locuzioni più generiche, parimenti idonee a consentire una puntuale valutazione del rischio, ma meno lesive dei princìpi di protezione dei dati.

Il Garante ha quindi disposto nei confronti della compagnia il blocco dell'ulteriore trattamento di tali dati nell'espletamento del servizio di fornitura telefonica di preventivi, prescrivendo al contempo la cancellazione di quelli relativi agli utenti per i quali non fossero stati completati i preventivi, la cui conservazione non è risultata giustificata in relazione alle esigenze prospettate dalla compagnia (art. 11, comma 1, lett. *e*), del Codice; *Provv.* 2 dicembre 2010 [doc. *web* n. 1780277]).

11.4. RAPPORTI DI LAVORO E PREVIDENZA

11.4.1. Rapporto di lavoro in ambito pubblico

Anche nel 2010, per dare riscontro a molteplici segnalazioni e quesiti di amministrazioni pubbliche, dipendenti e organizzazioni sindacali, sono state richiamate le "*Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*" (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In merito ad una richiesta di un'organizzazione sindacale di conoscere i nominativi del personale che aveva partecipato ad attività ispettive, il numero delle ispezioni ed i relativi corrispettivi, l'Ufficio ha ribadito che, salve puntuali previsioni normative o contrattuali, l'amministrazione può fornire alle oo.ss. solo dati numerici o aggregati (art. 19, comma 3, del Codice; punto 5.2. del cit. *provvedimento*) (*Nota* 12 aprile 2010).

In questi casi, come evidenziato dall'Ufficio in risposta ad un quesito riguardante l'accesso delle RSU alla documentazione concernente i debiti e i crediti orari, nonché i tabulati delle timbrature del personale amministrativo di una scuola, spetta all'amministrazione destinataria della richiesta valutare la sussistenza dell'interesse giuridicamente rilevante e le altre condizioni che legittimano l'accesso del richiedente, nonché le ragioni per le quali tali documenti possono essere sottratti alla sua conoscibilità, essendo l'amministrazione in possesso di tutti gli elementi di ponderazione necessari (*Nota* 21 aprile 2010).

Con riferimento alla segnalazione dell'avvenuta pubblicazione, su un periodico informativo di un comune, di alcuni dati personali dei singoli dipendenti dell'ente locale, riguardanti il rapporto di lavoro e lo stato di salute (tra cui trattamento economico, trattenute previdenziali, giorni di ferie, di malattia, permessi usufruiti ai sensi della l. n. 104/1992, assenze retribuite per maternità, congedo parentale e malattia figli), l'Ufficio ha evidenziato, in particolare, il divieto di diffondere dati idonei a rivelare lo stato di salute. Il Comune ha, al riguardo, assicurato che le future pubblicazioni sul proprio periodico saranno effettuate in conformità al vigente quadro normativo (art. 21, comma 1, l. 18 giugno 2009, n. 69; v. ora anche il comma 1-*bis*, introdotto dall'art. 5, comma 2, l. 4 novembre 2010, n. 183) (*Nota* 24 novembre 2010).

Sempre in materia di dati sensibili, in ottemperanza al *provvedimento* 21 ottobre 2009 [doc. *web* n. 1689440] (v. *Relazione* 2009, p. 164), il Ministero della difesa-Direzione generale per il personale militare ha adottato il 2 dicembre 2009 un decreto dirigenziale che, in particolare, dispone la cancellazione dalla documentazione sanitaria delle informazioni sullo stato di salute del personale, ad esclusione del giudizio medico-legale di idoneità al servizio, della riconducibilità dell'infermità a causa di servizio, della posizione di collocamento in congedo e dell'abilità a determinati impieghi. Più in generale, il

decreto vieta il trattamento di dati relativi allo stato di salute del personale che non siano indispensabili all'adozione dei provvedimenti di competenza.

Sono stati avviati dal Ministero della difesa approfondimenti, anche sulla base di indicazioni rese per le vie brevi dal Garante, in relazione alla prassi di comunicare all'autorità di pubblica sicurezza i nominativi dei militari affetti da patologie psiconeurologiche ai fini della revoca dell'autorizzazione di polizia a detenere armi a titolo privato.

Su eventuali proposte di modifica della normativa sull'ordinamento militare dovrà esprimersi l'Autorità ai sensi dell'art. 154, comma 4, del Codice (d.P.R. 15 marzo 2010, n. 90) (*Nota* 30 settembre 2010).

In argomento, si segnala da ultimo il d.lgs. 26 ottobre 2010, n. 204 il quale prevede che con decreto adottato dal Ministro della salute, di concerto con il Ministro dell'interno, sentito il Garante per la protezione dei dati personali, siano definite "*le modalità dello scambio protetto dei dati informatizzati tra il servizio sanitario nazionale e gli uffici delle forze dell'ordine nei procedimenti finalizzati all'acquisizione, alla detenzione ed al conseguimento di qualunque licenza di porto delle armi*" (art. 6).

A seguito di una segnalazione riguardante un bando di concorso del Ministero della difesa per allievi dell'Accademia navale, il quale aveva previsto l'esclusione dal concorso dei concorrenti al Corpo sanitario militare marittimo in caso di positività al *test HIV*, l'Ufficio ha avviato una serie di approfondimenti nei confronti dell'amministrazione della difesa per verificare le particolari cautele in materia di indagini volte ad accertare l'esistenza la sieropositività nei confronti di persone prese in considerazione per l'instaurazione di un rapporto di lavoro (artt. 5 e 6, l. 5 giugno 1990, n. 135; Corte costituzionale sentenza n. 218 del 1994; artt. 3, 11, 22, 112 e 184, comma 3, del Codice) (*Nota* 8 gennaio 2010).

Sono pervenute, inoltre, all'Autorità numerose segnalazioni riguardanti l'affidabilità degli strumenti telematici utilizzati dal Ministero per i beni e le attività culturali per la raccolta delle domande di partecipazione ad una procedura selettiva per restauratori e per l'iscrizione ad un elenco riguardante talune categorie di archeologi. Al riguardo il citato Ministero ha fornito idonee assicurazioni sulle misure adottate per garantire la protezione

dei dati personali raccolti, con particolare riferimento all'affidabilità dei siti Internet utilizzati (*Nota* 30 settembre 2010).

In un altro caso alcuni dipendenti hanno lamentato la pubblicazione, sul sito del Ministero della giustizia di alcuni provvedimenti, relativi all'inquadramento del personale e contenenti, tra l'altro, i codici fiscali dei dipendenti, accessibili anche tramite i comuni motori di ricerca. In proposito il Ministero ha dichiarato di aver effettuato la pubblicazione in ottemperanza a quanto previsto dall'art. 32 della l. 18 giugno 2009, n. 69 e di aver provveduto a cancellare i codici fiscali (*Nota* 10 novembre 2010).

11.4.2. Rapporto di lavoro in ambito privato

In una segnalazione un dipendente di una società aveva ritenuto illecita la richiesta che quest'ultima gli aveva rivolto di documentare (dal punto di vista sanitario) le "*improcrastinabili esigenze personali*" poste a fondamento dell'istanza di fruizione di un periodo feriale.

L'Autorità ha ritenuto ingiustificata la richiesta di documentazione in quanto, benché formulata nell'ambito di una legittima attività di verifica per finalità di gestione del rapporto di lavoro, non trovava giustificazione né nella normativa vigente (art. 2109 c.c.), né nella normativa contrattuale esaminata. Peraltro, la stessa richiesta non è risultata giustificata nemmeno in relazione alla finalità concretamente perseguita dalla società, tenuto conto della discrezionalità che la stessa normativa riconosce a quest'ultima nell'individuare il periodo di fruizione delle ferie da parte dei lavoratori (art. 2109 c.c.; art. 38 del CCNL applicabile).

Conseguentemente, è stato prescritto alla società di sensibilizzare i soggetti preposti a non chiedere la produzione di documenti volti a rendere note le ragioni delle richieste di congedo ordinario avanzate dai dipendenti (*Provv.* 4 novembre 2010 [doc. *web* n. 1779735]).

L'Autorità ha poi esaminato una richiesta di verifica preliminare formulata da una società (anche nell'interesse di altre controllate) che intendeva adottare uno strumento di valutazione dei dipendenti basato su procedure di autovalutazione e sui riscontri forniti dai terzi.

Il sistema, preordinato all'elaborazione dei dati acquisiti per il tramite di questionari compilati in forma anonima (successivamente "sintetizzati" e "aggregati" in *report* finali resi disponibili, tra l'altro, agli stessi interessati), sarebbe stato utilizzato su un numero ristretto di dipendenti (circa una ventina su base annua), anche in collegamento con il processo di valutazione del personale e per la corresponsione di eventuali incentivi economici. Inoltre, tale sistema avrebbe consentito ai lavoratori di valutare meglio le proprie capacità professionali e l'attività espletata, con significativi contributi al miglioramento delle prestazioni lavorative e al raggiungimento degli obiettivi concordati in sede aziendale. L'Autorità ha reputato il trattamento lecito e proporzionato, sia perché giustificato dalle specifiche dinamiche di tipo contrattuale presenti in ambito aziendale, sia perché effettuato su base meramente consensuale (art. 23 del Codice), senza pregiudizio per i lavoratori che avessero manifestato un eventuale diniego al trattamento, della possibilità di conseguire comunque un incentivo di natura economica.

L'Autorità ha tuttavia richiamato al rispetto di specifiche disposizioni (art. 14 del Codice; art. 8 della l. n. 300/1970), prescrivendo al contempo alla società di conservare i dati non oltre il termine strettamente necessario al perseguimento della finalità dichiarata (art. 11, comma 1, lett. *e*), del Codice) (*Provv.* 4 novembre 2010 [doc. *web* n. 1771838]).

A seguito di una segnalazione l'Autorità si è poi pronunciata sul trattamento di dati personali dei lavoratori svolto da una società mediante sistemi di localizzazione satellitare (*Provv.* 7 ottobre 2010 [doc. *web* n. 1763071]).

L'interessato aveva lamentato l'installazione, a bordo di alcuni autoveicoli in dotazione alla società presso la quale prestava servizio, di un sistema di localizzazione satellitare in assenza di preventiva informativa ai lavoratori e in asserita violazione della disciplina sul controllo a distanza dell'attività dei lavoratori (art. 4, comma 2, l. n. 300/1970).

L'Autorità, nel riconoscere che i dispositivi in esame servivano anche per pianificare gli interventi, diminuire i costi per danni conseguenti a violazioni del codice della strada, nonché per determinare i costi di trasferta e di intervento, e per esigenze di sicurezza sul lavoro, ha tuttavia evidenziato che il loro impiego deve comunque avvenire, oltre che in osservanza della pertinente disciplina di settore in tema di controlli a distanza, nel rispetto

dei princìpi in materia di protezione dei dati personali e con modalità concretamente idonee a garantire, in particolare, l'osservanza dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2 del Codice).

Le risultanze istruttorie hanno evidenziato che la società non aveva rispettato il precetto di cui all'art. 4, comma 2, della l. n. 300/1970; non aveva notificato il trattamento, né documentato la formale designazione quali incaricati del trattamento dei soggetti effettivamente legittimati ad accedere alle informazioni acquisite (art. 30 del Codice).

L'Autorità ha quindi disposto il blocco del trattamento nei confronti della società titolare; formulato al contempo –in caso di eventuale rilascio del provvedimento autorizzatorio da parte del competente ufficio territoriale del Ministero– specifiche prescrizioni in tema di notificazione del trattamento e di designazione degli incaricati, e infine, ha invitato la società commisurare i tempi di conservazione dei dati alle finalità concretamente perseguite.

Il trattamento dei dati personali dei dipendenti effettuato mediante strumenti di localizzazione satellitare è stato anche oggetto di una verifica preliminare richiesta da un'associazione operante nel campo dei controlli sulle aziende zootecniche per certificare l'effettività dei controlli svolti presso le aziende associate (in ottemperanza alle pertinenti normative di settore), e documentare la propria attività presso gli enti pubblici sovvenzionanti (in particolare, il Ministero delle politiche agricole, alimentari e forestali).

Il Garante ha ritenuto lecito il trattamento ove effettuato per la finalità dichiarata e nel rispetto delle prescrizioni di cui all'art. 4, comma 2, l. n. 300/1970; ha prescritto all'associazione di anonimizzare i dati di localizzazione in caso di loro comunicazione a terzi per dar conto dell'attività espletata, nonché di rendere agli interessati un'informativa dettagliata ed esaustiva circa il trattamento da svolgere. È stato infine prescritto all'associazione di provvedere alla notifica del trattamento (*Provv.* 18 febbraio 2010 [doc. *web* n. 1703103]).

A seguito di alcune notizie di stampa, l'Autorità ha valutato i trattamenti svolti da una società in relazione ai dati personali dei propri dipendenti, consistenti nell'utilizzo di "tagliandi" scritti a fini di allontanamento temporaneo dalla postazione di lavoro, per

assicurare al cliente una fornitura di prodotti continua e per garantire una efficace e tempestiva sostituzione dei dipendenti momentaneamente allontanatisi.

Il trattamento è stato tuttavia ritenuto lesivo della disciplina in materia di protezione dei dati personali ed è stato vietato alla società di trattare ulteriormente i dati dei lavoratori acquisiti per il tramite dei citati tagliandi scritti.

Al riguardo, il Garante ha rilevato che l'utilizzo dei tagliandi, per allontanamenti dei lavoratori dovuti all'espletamento di necessità "fisiologiche", risulta contrario all'art. 2 del Codice, soprattutto in considerazione del potenziale condizionamento (anche in termini di mortificazione personale) degli interessati in ordine alla propria libertà di movimento, nonché comunque sproporzionato e non necessario (artt. 3 e 11, comma 1, lett. *d*), del Codice).

Nel vietare il trattamento l'Autorità ha inoltre prescritto alla società di predisporre nuove modalità di comunicazione delle assenze temporanee dei dipendenti dalla propria postazione lavorativa, tali da assicurare l'effettiva salvaguardia della dignità e riservatezza dei lavoratori (*Provv.* 24 febbraio 2010 [doc. *web* n. 1705070]).

Cessione d'azienda: uso della casella di posta dell'ex dipendente

Con il *provvedimento* 22 aprile 2010 [doc. *web* n. 1727692], il Garante si è occupato di una particolare fattispecie: la cessione inter-societaria dell'azienda e, per quanto di competenza dell'Autorità, degli *account* di posta elettronica appartenenti al dominio aziendale.

Nel caso, due lavoratrici hanno lamentato l'utilizzo da parte della società, acquirente del compendio fallimentare, degli indirizzi di posta elettronica aziendale loro assegnati.

In particolare, le segnalanti hanno evidenziato la possibilità che la società subentrante non avesse disattivato i rispettivi *account* di posta elettronica (dal momento che le comunicazioni inviate non generavano messaggi di errore) rappresentando quindi il rischio che la suddetta società potesse leggere le e-mail pervenute sui propri indirizzi.

La società ha ammesso di utilizzare le caselle di posta elettronica delle segnalanti, precisando di aver adottato la modalità "*catch-all*", tale da consentire la ricezione di tutti i messaggi pervenuti sugli indirizzi appartenenti al dominio aziendale in maniera indifferenziata su un'unica casella di posta elettronica.

La società ha sottolineato che tale scelta era stata giustificata dalla circostanza dell'avvenuto acquisto dell'intero compendio fallimentare della società cedente, incluso il

relativo avviamento e, quindi, anche il dominio aziendale, ivi compresi gli indirizzi di posta elettronica aziendale, nonché dalla circostanza che l'utilizzo di questi ultimi risultasse indispensabile alla corretta gestione dei rapporti commerciali della società.

Ciò in considerazione del fatto che le segnalanti avrebbero svolto, anche successivamente alla cessione aziendale, un'attività di sviamento della clientela.

La società ha rappresentato altresì come le segnalanti risultassero socie di una nuova società, dalla denominazione simile a quella della società cedente, costituita poco dopo la dichiarazione di fallimento.

Il Tribunale di Bologna, adito sulla questione, aveva dato atto che la ricezione dei dati da parte della stessa avveniva in modo indifferenziato secondo il *cd.* "sistema del *catch-all*", che non consentiva di risalire al destinatario, e che inoltre le caselle in questione erano di pertinenza aziendale con conseguente proprietà delle stesse da parte dell'imprenditore e possibilità dello stesso di accedervi.

Il Garante, tuttavia, considerando l'esigenza di tutela dei dati personali in rilievo, con il citato *provvedimento*, ha prescritto alla società subentrata nella titolarità degli indirizzi in questione la disattivazione di tutti gli *account*, appartenenti al dominio aziendale, ma attribuiti personalmente a soggetti che non facevano più parte dell'organizzazione imprenditoriale della società e la predisposizione di un sistema idoneo ad informare della disattivazione tutti i mittenti di comunicazioni inviate agli *account*, invitando all'inoltro della corrispondenza di lavoro ad un indirizzo di posta elettronica alternativo.

11.4.3. Previdenza

Un cittadino aveva segnalato al Garante di aver ricevuto dall'INPS un plico che presentava, sulla parte esterna, indicazioni relative alla copia, ivi contenuta, di un verbale di accertamento dell'invalidità civile. Al riguardo, l'Ufficio ha evidenziato che i plichi postali non devono recare, sulla parte esterna, indicazioni da cui possano evincersi, in modo esplicito, informazioni idonee a rivelare lo stato di salute dell'interessato (artt. 11 e 22, comma 3, del Codice) (*Nota* 23 luglio 2010).

Nel corso del 2010 sono proseguite le attività di controllo avviate nell'anno precedente

sui sistemi informativi dell'INPS. In particolare, gli approfondimenti ispettivi hanno riguardato la conformità alla disciplina sulla protezione dei dati personali degli accessi alle banche dati dell'Istituto effettuati da soggetti esterni, specie in relazione alle finalità istituzionali perseguite, alle tipologie di dati trattati e alle modalità di trattamento. All'esito di taluni accertamenti effettuati *in loco* sui sistemi informativi dell'INPS, a seguito di controlli avviati negli anni precedenti, l'Ufficio ha chiesto all'Istituto informazioni relative: ai sistemi di autenticazione ed autorizzazione degli applicativi utilizzati dai soggetti esterni; al sistema di gestione telematica della procedura di riconoscimento dei benefici in materia di invalidità civile, cecità civile, sordità civile, *handicap* e disabilità; alle modalità di comunicazione all'Istituto delle variazioni anagrafiche da parte degli enti locali; al funzionamento del "casellario pensioni" e alla banca dati contenente le attestazioni ISEE (*Nota* 23 dicembre 2010).

Una direzione provinciale dell'INPS ha informato l'Autorità, ai sensi degli artt. 19 e 39 del Codice, di voler trasmettere ad un istituto autonomo case popolari i dati personali relativi agli importi delle pensioni e degli assegni sociali erogati dall'INPS in favore dei componenti i nuclei familiari assegnatari di alloggi, per consentire allo stesso IACP di verificare le autocertificazioni degli interessati sulla loro situazione reddituale. Al riguardo l'Ufficio ha rappresentato che, in particolare, ove il flusso di dati personali trovi la propria fonte nelle norme che impongono di controllare la veridicità delle dichiarazioni sostitutive, non occorre effettuare alcuna comunicazione al Garante. Ciò fermo restando il rispetto dei princìpi di pertinenza e non eccedenza dei dati oggetto di comunicazione, nonché delle modalità e dei limiti dei controlli stabiliti dalle medesime disposizioni (art. 11, comma 1, lett. *d*), del Codice e artt. 43, 46 e 71 del d.P.R. 28 dicembre 2000, n. 445) (*Nota* 28 gennaio 2010).

In relazione ad un progetto finalizzato all'assistenza di lavoratori esposti all'amianto, l'INPS ha comunicato all'Autorità, ai sensi dell'art. 39 del Codice, di voler trasmettere ad un'azienda sanitaria della Regione Friuli Venezia Giulia taluni dati personali relativi agli occupati in aziende operanti in determinate zone del territorio regionale. Al riguardo, l'Ufficio ha evidenziato che la speciale disciplina prevista dall'art. 39 del

Codice riguarda esclusivamente comunicazioni di dati non sensibili. La comunicazione prospettata dall'INPS può, dunque, essere effettuata soltanto nella misura in cui non si tratti di dati idonei a rivelare lo stato di salute degli interessati (quali, ad es., quelli riguardanti i lavoratori esposti richiedenti il riconoscimento dei benefici connessi a tale esposizione ai sensi dell'art. 13 della l. 27 marzo 1992, n. 257 oppure il riconoscimento di malattie professionali). Con riferimento, inoltre, alla prospettata interconnessione dei suddetti dati con ulteriori informazioni, anche di carattere sensibile detenute da altri soggetti pubblici, l'Ufficio ha evidenziato la necessità di individuare con chiarezza le finalità perseguite, di verificare l'esistenza di idonei presupposti giuridici (artt. 20 e 22, comma 11, del Codice) e di rispettare il pertinente quadro normativo di settore (art. 244, d.lgs. 9 aprile 2008, n. 81; d.P.C.m. 10 dicembre 2002, n. 308; l.r. 12 settembre 2001, n. 22) (*Nota* 10 dicembre 2010).

11.5. ALTRE ATTIVITÀ IMPRENDITORIALI

Rientra in questo settore una eterogenea casistica, di seguito esposta in sintesi.

Per facilitare la consultazione dei dati degli iscritti nelle graduatorie ad esaurimento del personale docente pubblicate sui siti *web* degli uffici scolastici provinciali del Ministero della pubblica istruzione, una società ha chiesto al Garante di essere esonerata dall'obbligo di rendere l'informativa.

Il Garante ha accolto l'istanza di esonero formulata dalla società per la ritenuta impossibilità di rilasciare l'informativa individuale a tutti gli interessati (pari a circa 300.000 unità), nonché in considerazione dell'utilità sociale rivestita dal progetto e delle specifiche previsioni in materia (che facoltizzano i soggetti privati, nei termini e alle condizioni ivi previste, a riutilizzare le informazioni del settore pubblico per finalità anche commerciali; art. 2, comma 1, lett. *e*), del d.lgs. n. 24 gennaio 2006, n. 36).

L'Autorità ha comunque prescritto alla società di pubblicare sul proprio sito *web* un'idonea e preventiva informativa a vantaggio di tutti i docenti interessati, dalla quale emergano le puntuali caratteristiche del trattamento effettuato in ordine ai loro dati personali (*Provv.* 26 marzo 2010 [doc. *web* n. 1721169]).

In un altro caso, l'Autorità è stata chiamata a pronunciarsi sul trattamento effettuato da una società relativamente alle richieste di assistenza formulate dagli utenti per il tramite del relativo *call center*.

Il segnalante, in particolare, aveva lamentato che la società cui si era rivolto per ricevere informazioni generiche sui centri di assistenza autorizzati alla riparazione della sua stampante subordinava il rilascio di dette informazioni alla preventiva acquisizione dei dati personali del chiamante e al rilascio del consenso al relativo trattamento.

Al riguardo, l'Autorità ha ritenuto sproporzionata l'acquisizione di dati personali diversi dal nome e cognome del chiamante nella fase antecedente l'intervento di assistenza telefonica, talora, in astratto, potenzialmente risolutivo del problema. Viceversa, la raccolta di altri dati (indirizzo; numero di telefono; indirizzo di posta elettronica) è stata ritenuta lecita se effettuata in un momento successivo, qualora si dovesse rendere necessaria la predisposizione di misure alternative all'assistenza telefonica (ad. es, per l'organizzazione di interventi a domicilio).

L'Autorità ha pertanto vietato alla società di trattare ulteriormente i predetti dati nella fase antecedente l'intervento di assistenza tecnica (*Provv.* 4 marzo 2010 [doc. *web* n. 1721214]).

Una volontaria *Caritas* aveva segnalato all'Autorità che, accompagnando una portatrice di *handicap* a fare la spesa presso un punto vendita di una nota catena commerciale di supermercati, aveva constatato che per il servizio di consegna a domicilio gratuito riservato agli invalidi al 100%, veniva richiesta copia del verbale di invalidità, tanto che un'addetta all'esercizio commerciale aveva rifiutato all'interessata di poter fruire del servizio sulla base della mera esibizione di una tessera attestante lo stato di invalidità, affermando che, al contrario, era indispensabile acquisire copia del predetto verbale.

Il Garante ha reputato sproporzionata la richiesta di esibire copia del verbale rilasciato, tenuto conto della pluralità di informazioni in esso contenute e, in particolare, del giudizio diagnostico espresso dalla Commissione medica. L'Autorità ha pertanto vietato ulteriori richieste di esibizione del verbale e ha invitato la società a riformulare l'informativa resa alla clientela interessata alla tipologia di trattamenti in esame, carente

di talune indicazioni richieste dall'art. 13 del Codice (*Provv.* 13 maggio 2010 [doc. *web* n. 1729156]).

A seguito di un procedimento su ricorso, l'Autorità si è poi pronunciata sul trattamento di dati personali effettuato da una società di autonoleggio.

Dalla documentazione acquisita era emerso che la società, nell'ambito di un contratto stipulato con l'interessato, aveva comunicato alcuni suoi dati personali ad altra società (proprietaria del veicolo noleggiato) affinché la stessa potesse notificargli il verbale di contestazione di una violazione alle norme del codice della strada.

L'Autorità, alla luce degli elementi acquisiti, non ha ritenuto lecito il trattamento svolto posto che il riferimento della società di autonoleggio al codice della strada e ad obblighi contrattuali nei confronti della società proprietaria del veicolo non è risultato pertinente; inoltre, non è risultato acquisito il consenso dell'interessato a tale specifico trattamento, né è stata addotta dalla società l'esistenza di altro presupposto di liceità (artt. 23 e 24 del Codice).

È stato inoltre prescritto alla società di riformulare l'informativa da rendere alla clientela, atteso che quella prodotta agli atti non è risultata conforme all'art. 13 del Codice (*Provv.* 16 giugno 2010 [doc. *web* n. 1741982]).

Trattamento per finalità di *marketing* di dati personali contenuti nel Pubblico registro automobilistico

In numerosi quesiti e segnalazioni riguardanti l'utilizzabilità, da parte di operatori economici privati, dei dati personali contenuti nel Pubblico registro automobilistico (PRA) gli utenti lamentavano di aver ricevuto, da società private, alle quali non avevano mai comunicato il proprio recapito, comunicazioni pubblicitarie, offerte d'intervento per effettuare la revisione della propria vettura o questionari con finalità di ricerca statistica.

Con *provvedimento* 11 marzo 2010 [doc. *web* n. 1709295], in base al quadro normativo di riferimento (r.d.l. 15 marzo 1927, n. 436; r.d. 29 luglio 1927, n. 1814; l. 9 luglio 1990 n. 187; d.m. 514 del 1992), l'Autorità ha affermato che l'accesso al PRA delle società di *direct marketing* per acquisire dati a fini di invio di proposte commerciali non é risultato compatibile con gli scopi per i quali la normativa prevede la raccolta dei dati (art. 11, comma 1, lett. *b*), del Codice).

Il Pubblico registro automobilistico, infatti, è stato istituito (r.d.l. 15 marzo 1927) per assicurare un regime di pubblicità legale con riguardo al trasferimento della proprietà e ai

vincoli di privilegio costituiti sugli autoveicoli, nonché per fornire quelle informazioni sui veicoli che possono risultare utili a fini di "interesse pubblico".

Pertanto, per quanto pubblici (art. 24 del Codice), i dati contenuti nel PRA non possono essere utilizzati, in assenza di un preventivo consenso, per scopi unicamente commerciali o pubblicitari, essendo tali finalità incompatibili con il sistema di pubblicità legale cui il registro è preordinato e, al contempo, avulse da qualsiasi rilevante interesse sociale comunque richiesto dalla norma.

L'Autorità ha invece considerato legittimo l'utilizzo, anche senza consenso, dei dati personali contenuti nel PRA da parte delle società (o centri) di revisione e delle officine autorizzate, per inviare questionari o comunicazioni relativi all'imminente scadenza del periodo di revisione dell'auto.

Ha infatti ravvisato, in tali casi, la sussistenza di un rilevante interesse pubblico a far conoscere informazioni che contribuiscono a migliorare la sicurezza nella circolazione degli autoveicoli e a favorire la tutela ambientale.

Tale interpretazione risulta altresì suffragata dal fatto che l'ACI, in occasione della redazione del proprio regolamento per l'accesso ai dati del PRA (dapprima emanato ai sensi dell'art. 23, comma 4, del citato d.m. 2 ottobre 1992, n. 514 e successivamente modificato ed integrato il 19 giugno 2002, anche al dichiarato fine di adeguarne il contenuto alla l. n. 675/1996, *medio tempore* entrata in vigore) ha confermato che, tra le categorie di utenti che abbiano un rilevante interesse a conoscere i dati registrati nel PRA, vanno annoverate anche "le società del settore automobilistico", tra cui possono ricomprendersi anche i *cd.* "*centri di revisione*" (art. 3, lett. *d*), del predetto regolamento).

Autorizzazione al trattamento dei dati giudiziari da parte di società di revisione contabile

Sono state sottoposte all'esame dell'Autorità alcune richieste di autorizzazione al trattamento dei dati giudiziari relativi, in particolare, a clienti, soci e dirigenti di alcune società di revisione contabile. Tali richieste, tutte di analogo tenore, venivano giustificate dalle società istanti in base al quadro normativo statunitense (il *Sarbanes-Oxley Act* del 2002), che impone alle società di revisione contabile che svolgono prestazioni professionali in favore di società emittenti azioni o prodotti finanziari soggetti al controllo della *U.S. Securities and Exchange Commission* di comunicare al *Public Company Accounting*

Oversight Board –organismo istituito con finalità di monitoraggio, tra l'altro, delle medesime società di revisione– alcune informazioni concernenti eventuali procedimenti penali a carico dei soggetti sopra indicati, pena l'impossibilità di registrarsi presso lo stesso PCAOB e, conseguentemente, di svolgere la propria attività di revisione; tanto, muovendo dall'assunto, peraltro corretto, che non potesse trovare applicazione alla fattispecie in esame l'autorizzazione generale n. 7/2009.

L'Autorità, ha rigettato le istanze, poiché il trattamento di dati giudiziari oggetto delle richieste avrebbe determinato un conflitto tra la disciplina nazionale e comunitaria e la stessa normativa statunitense; tra l'altro lo stesso *Sarbanes-Oxley Act* prevede la possibilità di esentare le società non statunitensi dall'applicazione della normativa ivi contenuta, qualora il conferimento di determinate informazioni al *Public Company Accounting Oversight Board* nella procedura di registrazione possa violare una legge nazionale non statunitense (*provvedimenti* 3 giugno 2010 [doc. *web* nn. 1737838; 1737844; 1738372; 1737997; 1738015; 1738024; 1738030; 1738053]).

11.6. TRATTAMENTO DI DATI PER LA "TESSERA DEL TIFOSO"

Il Garante ha valutato la liceità di taluni trattamenti di dati personali svolti nella realizzazione del programma "tessera del tifoso" varato dall'Osservatorio nazionale sulle manifestazioni sportive-Dipartimento della pubblica sicurezza del Ministero dell'interno, a seguito di alcune istanze relative, in particolare a: l'assenza di un'idonea base giuridica in grado di giustificare l'obbligo di sottoscrizione della tessera; l'inidoneità dell'informativa presente sui moduli predisposti dalle società; l'inadeguatezza della stessa modulistica utilizzata per il rilascio della tessera; l'assenza di una "copertura" normativa relativamente al connesso trattamento di dati giudiziari; il rischio di profilazione degli utenti derivante dalle finalità di *marketing* connesse all'impiego della tessera; l'utilizzo di tecnologia *RFID* per scopi non chiaramente individuati, né previamente indicati all'utenza (*Provv.* 10 novembre 2010 [doc. *web* n. 1779725]).

All'esito dell'istruttoria il Garante ha ritenuto che, allo stato, non difetterebbero idonei presupposti normativi atti a giustificare il trattamento dei dati personali (anche giudiziari)

connesso all'adozione della tessera del tifoso, tenuto conto dell'inquadramento giuridico –eventualmente sindacabile in altra sede– già riconosciuto allo strumento dallo stesso Ministero dell'interno (secondo cui la tessera costituirebbe una "facilitazione" ai sensi dell'art. 8 del d.l. n. 8/2007). La mancata acquisizione, in sede di adesione al programma "tessera del tifoso", del consenso degli interessati relativamente alla gestione del rapporto in corso di instaurazione è risultata giustificata considerando il trattamento necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato (art. 24, comma 1, lett. *b*), del Codice). Sotto distinto profilo, non è risultato invece provato il rischio di localizzazione degli utenti in ragione del *chip* a tecnologia *RFID* presente sulla tessera, tenuto conto che quest'ultima è risultata leggibile dagli appositi dispositivi esclusivamente ad una distanza ravvicinata (non superiore ai 10 cm). Ciò, muovendo dall'ulteriore presupposto, di carattere più generale, che lo stesso trattamento correlato all'impiego di tecnologia *RFID* per finalità di accesso agli impianti sportivi è risultato necessario e non eccedente, attese anche le garanzie offerte sul piano della sicurezza e della velocizzazione degli accessi (avuto riguardo altresì all'elevato numero di spettatori presente, di solito, sugli spalti).

Per altro verso, il Garante ha invece riscontrato alcune "criticità" relativamente all'informativa resa agli interessati, all'acquisizione del loro consenso per finalità di *marketing*, alla qualificazione dei rapporti intercorrenti tra i soggetti coinvolti nell'iniziativa.

L'Autorità ha dunque prescritto alle società sportive coinvolte nel programma "tessera del tifoso" di integrare, ove necessario, l'informativa da rendere agli interessati e di predisporre moduli di adesione che consentano agli interessati di formalizzare anche il proprio diniego all'eventuale trattamento per finalità di *marketing*, anche da parte di società terze.

Le società sportive, inoltre, sono state invitate a valutare l'opportunità di predisporre moduli separati per ulteriori usi della tessera, per facilitare la comprensione delle caratteristiche e delle operazioni di trattamento effettuate dai soggetti coinvolti a vario titolo nell'iniziativa. Si è inoltre provveduto a richiamare l'attenzione delle società, ove interessate allo svolgimento di eventuali attività di profilazione, sulla necessità di acquisire un consenso specifico e distinto da parte degli interessati, nonché sulla necessità di provvedere alla notificazione del relativo trattamento (art. 37 del Codice).

Infine, è stato rivolto un invito affinché i soggetti che fossero risultati privi di reale e autonoma capacità decisionale in ordine alle finalità e modalità del trattamento fossero designati quali responsabili ai sensi dell'art. 29 del Codice.

L'Autorità, che si è riservata ulteriori iniziative e determinazioni (anche alla luce di eventuali revisioni apportate al programma dall'Osservatorio), ha conclusivamente prescritto alle società sportive di disporre la pubblicazione del *provvedimento* sui propri siti *web* (ove esistenti) al fine di favorirne una immediata consultazione da parte degli utenti.

12. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

La materia dei trasferimenti transfrontalieri di dati personali è stata oggetto di costante attenzione nel corso del 2010 con riferimento sia alla attiva partecipazione del Garante ai lavori del Gruppo Art. 29, sia al rilascio di autorizzazioni al trasferimento dei dati verso Paesi terzi, in particolare tramite "*Binding Corporate Rules*" (*BCR*) ("*Norme vincolanti d'impresa*").

In merito, diversi contributi sono stati apportati nell'ambito del sottogruppo *BCR*, per promuovere una maggiore trasparenza verso l'esterno (attraverso la proposta di pubblicare sul sito della Commissione europea, una pagina *web* contenente le principali informazioni relative alla fase europea di approvazione delle *BCR* e alle modalità e ai tempi per ottenere le relative autorizzazioni nazionali) ed estendere progressivamente la platea delle Autorità aderenti al meccanismo di *cd.* "*mutuo riconoscimento*", giunte attualmente a quota 19. Tale sistema, volto ad accelerare i tempi della procedura europea di cooperazione, ha comportato nell'ultimo anno considerevoli vantaggi, attraverso la definizione in tempi rapidi di diverse procedure europee di approvazione delle *BCR*.

Il lavoro del sottogruppo si è inoltre rivolto alla definizione di un documento ad uso interno delle Autorità per fornire una comune interpretazione degli aspetti maggiormente problematici collegati alla valutazione di adeguatezza delle norme vincolanti d'impresa, e semplificare l'analisi delle bozze di *BCR* da parte della *lead Authority*, costituendo un valido ausilio nell'ambito della procedura di mutuo riconoscimento.

Nel documento relativo alle "*standard contractual clauses*" (clausole contrattuali tipo) (WP 176 del 12 luglio 2010), redatto con l'attiva partecipazione di questa Autorità, sono stati forniti chiarimenti sui principali dubbi interpretativi espressi dagli operatori del settore nella fase di prima applicazione della Decisione della Commissione n. 2010/87/EU del 5 Febbraio 2010 (v. *infra* par. 20.2.).

L'attività del Garante è stata intensa anche a livello nazionale. La citata Decisione n. 2010/87/EU in materia di clausole contrattuali tipo è stata oggetto nel maggio 2010 di attuazione nell'ordinamento italiano, mediante specifica autorizzazione (*Provv.* 27 maggio 2010 [doc. *web* n. 1728496]). Il documento autorizza, con effetto dal 15 maggio 2010,

i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea (da titolare a responsabile) effettuati in conformità ad un nuovo schema di clausole contrattuali tipo, recante al proprio interno una clausola di "*subcontratto*" (v. *Relazione* 2009, p. 189). Al contempo, con tale autorizzazione il Garante ha raccolto l'invito della Commissione ad estendere l'applicazione del nuovo *set* di clausole contrattuali tipo anche a responsabili stabiliti in UE, che affidino il trattamento a subincaricati stabiliti in un Paese terzo, prevedendo, in capo al titolare del trattamento, l'obbligo di comunicare al Garante l'avvenuta designazione in successione di più di un subincaricato del trattamento (v. Decisione della Commissione n. 2010/87/UE, considerando 23).

Con riferimento al settore delle *BCR* l'Autorità, con i provvedimenti dell'8 aprile 2010 [doc. *web* n. 1717863] e del 7 ottobre 2010 [doc. *web* n. 1763052], si è pronunciata per la prima volta in ordine ad alcuni progetti di norme vincolanti d'impresa elaborati da importanti gruppi societari di carattere multinazionale.

Nel primo caso, l'istanza di autorizzazione è stata presentata da un gruppo multinazionale statunitense operante nel settore della ristorazione alberghiera, a seguito della conclusione, da parte della *lead Authority* (Autorità di protezione dei dati personali del Regno Unito di Gran Bretagna e Irlanda del Nord-*Information Commissioner's Office*), del procedimento di cooperazione europea instauratosi secondo il sistema di mutuo riconoscimento. La richiesta riguardava i trasferimenti intragruppo dei dati personali relativi ai dipendenti e alla clientela dal territorio dello Stato italiano, verso le filiali con sede in Paesi non appartenenti all'Unione europea.

Il Garante, a seguito di una complessa istruttoria, nel corso della quale ha preso atto delle dichiarazioni integrative rese dalla richiedente alla stessa Autorità (relative in particolare al contenuto e all'efficacia vincolante della clausola di responsabilità e del terzo beneficiario, nonché all'esatta portata dell'obbligo di adempimento delle misure di sicurezza prescritte dalla legge), ha autorizzato il trasferimento summenzionato secondo le modalità fissate nelle *BCR*, per il perseguimento delle sole finalità ivi dichiarate.

Il Garante ha comunque ribadito il proprio potere di svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su

ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, eventuali provvedimenti di blocco o di divieto. Infine, ha precisato che le operazioni di trattamento dei dati personali, anche se poste in essere a seguito del rilascio dell'autorizzazione, saranno lecite solo ove conformi alla normativa nazionale vigente e alle sue successive modificazioni, anche in materia di protezione dei dati personali, con particolare riferimento alle specifiche disposizioni sui presupposti di legittimità delle attività di raccolta dei dati oggetto del trasferimento e sulla sussistenza dei presupposti di legittimità per la comunicazione dei dati medesimi.

Di analogo tenore l'autorizzazione nazionale adottata dal Garante il 7 ottobre 2010, a seguito della definizione di una procedura di cooperazione europea attivata secondo le forme previste dal WP 107, nei confronti di un importante gruppo statunitense operante nel settore bancario e finanziario.

L'istanza aveva ad oggetto il trasferimento infragruppo, verso Paesi terzi, dei dati personali relativi al personale, anche interinale, ai fornitori, ai clienti, anche potenziali, ai referenti presso clienti aziendali, alle controparti, ai consorziati e altri operatori del mercato, nonché ai subappaltatori, per le finalità connesse alla gestione del rapporto di lavoro e alle operazioni svolte dalle società nell'esercizio della propria attività.

Anche in questo caso il Garante ha effettuato una complessa istruttoria, chiedendo opportuni chiarimenti in merito all'individuazione dei soggetti coinvolti nel trasferimento intragruppo dei dati verso Paesi terzi, all'ambito di applicazione delle clausole di responsabilità e del terzo beneficiario, alle definizioni contenute nel testo, ai diritti dell'interessato e all'esatta indicazione della tipologia dei dati personali oggetto delle *BCR*. L'autorizzazione è stata rilasciata nei limiti delle modalità di trasferimento indicate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate.

Privacy e agenzie di *rating*: maggiori controlli sui conflitti di interesse

Con riguardo al delicato tema del conflitto di interesse e del connesso trattamento di dati personali, il Garante è intervenuto con una importante decisione nel corso del 2010, che ha tratto origine dalla richiesta della filiale italiana di un'agenzia di *rating* statunitense di poter consultare, sulla base di una specifica *policy* interna aziendale, le informazioni relative alle operazioni su strumenti finanziari eseguite dai propri dipendenti e dai soggetti

facenti parte del loro nucleo familiare ristretto. Senza tali controlli, infatti, la società capogruppo, che opera in tutto il mondo, non avrebbe potuto ottemperare alla normativa vigente negli Stati Uniti, che richiede di certificare che l'attività di *rating* venga svolta in modo indipendente e senza essere influenzata da alcun conflitto di interessi anche dalle relative società controllate e/o collegate.

Nell'istruttoria, l'Autorità ha tenuto conto della recente normativa europea sul tema (*Regolamento* (CE) n. 1060/2009 del Parlamento europeo e del Consiglio del 16 settembre 2009, relativo alle agenzie di *rating* del credito), volta a migliorare, in particolare, la trasparenza, la responsabilità e l'affidabilità delle attività di *rating* del credito nella Comunità, per garantire un buon funzionamento del mercato interno e, al contempo, raggiungere un elevato grado di protezione degli investitori. È risultato necessario bilanciare la tutela della *privacy* con altre finalità di rilevante interesse pubblico quali l'indipendenza, l'oggettività e la qualità dei *rating* utilizzati nella Comunità, nonché la prevenzione di situazioni di conflitto di interesse. Pertanto, il Garante ha stabilito che la società potrà raccogliere e utilizzare i dati relativi agli strumenti finanziari, e alle operazioni ad essi connesse, di cui risultino detentori i dipendenti purché le informazioni, oggetto di trattamento, attinenti alle circostanze economiche e personali relative a tali soggetti, siano limitate all'accertamento della sussistenza dell'ipotetico conflitto di interessi (art. 11, comma 1, lett. *a*) e *b*), del Codice). L'Autorità ha inoltre precisato che tali dati potranno essere trattati per il perseguimento della sola predetta finalità e, comunque, nel rispetto dei princìpi e dei limiti stabiliti dalla normativa comunitaria vigente, anche con riferimento all'individuazione dei soggetti appartenenti al *cd.* "nucleo familiare ristretto", i quali dovranno essere ricondotti alle figure indicate nell'art. 1, par. 2 della Direttiva n. 2004/72/CE del 29 aprile 2004. L'agenzia di *rating*, inoltre, dovrà fornire a tutti gli interessati un'adeguata e puntuale informativa separatamente dalla relativa *Policy* aziendale e in lingua italiana. Infine, l'Autorità ha sottolineato che qualunque dato trattato dalla società in violazione della disciplina sulla *privacy* non potrà essere utilizzato (*Provv.* 19 maggio 2010 [doc. *web* n. 1736161]).

13. LIBERE PROFESSIONI

13.1. ORDINI PROFESSIONALI

Nel corso del 2010 sono pervenuti al Garante diversi quesiti concernenti, in particolare, il regime di conoscibilità delle informazioni relative agli iscritti agli albi.

Al riguardo, in termini generali, è stato ribadito che la diffusione dei dati degli iscritti ad un ordine professionale deve essere valutata in concreto dal relativo consiglio, in considerazione delle specifiche forme di pubblicità previste dalla normativa di settore.

Più in dettaglio, un consiglio nazionale aveva chiesto se fosse possibile, per esigenze di trasparenza, pubblicare sul proprio sito *web* i nominativi degli iscritti all'ordine destinatari di una sanzione disciplinare definitiva.

In proposito è stato evidenziato che può essere "*menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio delle professione*", purché il trattamento riguardi informazioni corrette, complete ed aggiornate (art. 11, comma 1 e 61, comma 2, del Codice; *Provv.* 29 marzo 2001 [doc. *web* n. 39536]; *Relazione* 2003, p. 82) (*Nota* 18 gennaio 2010).

È stato evidenziato ad un ordine professionale, in merito alla possibilità di diffondere gli indirizzi di posta elettronica degli iscritti, che una specifica recente normativa di settore prevede che i professionisti iscritti in albi ed elenchi debbano comunicare ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica (*Nota* 30 luglio 2010).

In termini analoghi si è risposto ad un avvocato che lamentava la pubblicazione sull'albo, in particolare, del suo codice fiscale (prevista dall'art. 3-*bis* del d.l. 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla l. 22 febbraio 2010, n. 24) (*Nota* 31 marzo 2010).

14. Trattamento dei dati personali in ambito condominiale

In questa materia, nella quale la casistica è di significativa rilevanza, si menziona un ricorso nel quale si lamentava l'affissione in spazi condominiali accessibili a terzi, di documenti contenenti dati personali riferiti all'istante (e, segnatamente, di una comunicazione avente ad oggetto la convocazione di un'assemblea straordinaria e di una copia del ricorso introduttivo che la ricorrente aveva proposto nei confronti di una delibera condominiale), in seguito rimossi. Si lamentavano, altresì, nuove affissioni nella bacheca, recanti la ripartizione delle spese sostenute dai singoli partecipanti (nominativamente identificati) in ambito condominiale.

L'Autorità ha ritenuto fondate le doglianze, per violazione, oltre che del principio di necessità (art. 3, del Codice), delle disposizioni in tema di pertinenza e non eccedenza dei dati trattati (artt. 3, 11, comma 1, lett. *d*), del Codice), evidenziando che le finalità perseguite avrebbero potuto essere ugualmente perseguite omettendo i riferimenti all'interessata e, comunque, ricorrendo a modalità alternative di comunicazione con gli altri partecipanti al condomino (cfr. *Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]). In mancanza del consenso dell'interessata alla divulgazione dei suoi dati personali, il trattamento è stato ritenuto illecito, con prescrizione al condominio di adottare opportune misure volte a conformarlo alla disciplina di protezione dei dati personali (*Provv.* 8 luglio 2010 [doc. *web* n. 1741950]).

Il Garante si è poi pronunciato in ordine alla liceità del trattamento operato da una società a responsabilità limitata (nella sua qualità di amministratore di un condominio) conseguente all'avvenuta partecipazione di alcuni suoi soci alle assemblee condominiali.

Al riguardo, l'Autorità ha precisato che il trattamento svolto nel caso di specie non poteva considerarsi lecito, posto che tra i poteri dei soci legislativamente (art. 2479 c.c.) e statutariamente (art. 11 dei patti sociali) previsti non figurava il diretto e personale espletamento di attività attuative dell'oggetto sociale (l'amministrazione dei condomini e la gestione dei servizi comuni relativi agli immobili); al contrario, dal materiale documentale acquisito agli atti è emerso che l'unico soggetto concretamente legittimato ad amministrare

e rappresentare il condominio (perseguendo, così, l'oggetto sociale della società) risultava, in base alla legge, all'atto costitutivo e ai patti sociali, l'amministratore unico della società. Inoltre, non è risultato provato che la partecipazione in assemblea dei predetti soci fosse stata ritenuta necessaria dagli stessi partecipanti all'assemblea condominiale.

Il Garante ha dunque prescritto alla società, nella sua dichiarata veste di titolare del trattamento, di adottare idonee misure organizzative tese a prevenire la partecipazione alle assemblee del condominio di soggetti non effettivamente legittimati (*Provv.* 9 settembre 2010 [doc. *web* n. 1758751]).

15. La videosorveglianza e la biometria

15.1. Videosorveglianza in ambito pubblico

Nel 2010 il Garante è stato più volte chiamato a fornire chiarimenti sul nuovo *provvedimento* generale adottato in materia di videosorveglianza (*Provv.* 8 aprile 2010 [doc. *web* n. 1712680], in *G.U.* 29 aprile 2010, n. 99; *Relazione* 2009, p. 25 ss.).

Conformemente a quanto già registrato in questa sede da alcuni anni, anche quest'anno molti comuni, dopo aver adottato uno specifico *provvedimento* per disciplinare le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio, lo avevano trasmesso al Garante per ottenerne l'approvazione ovvero solo per darne conoscenza. Al riguardo, è stato ribadito che l'installazione di tali sistemi non deve essere sottoposta all'esame preventivo del Garante, fatte salve le specifiche ipotesi per le quali è necessario richiedere una verifica preliminare, e che non può desumersi alcuna approvazione implicita dal silenzio del Garante dopo la ricezione di documenti relativi a progetti di videosorveglianza (punti 3.2.1. e 3.2.2. del cit. *provvedimento* generale; art. 17 del Codice) (*Note* 9 giugno; 18 giugno; 9 luglio; 23 agosto; 25 ottobre; 4 novembre; 15 novembre; 22 novembre e 24 novembre 2010).

Chiarimenti circa l'applicazione del nuovo *provvedimento* del Garante in materia di videosorveglianza sono stati, altresì, richiesti da numerosi comuni all'Associazione nazionale comuni italiani (ANCI), che ha ritenuto opportuno predisporre delle apposite linee-guida, invitando l'Autorità a collaborare al fine di fornire adeguate indicazioni per l'installazione e la gestione di telecamere e sistemi di controllo video anche a fini di sicurezza urbana.

Un'università, un'azienda sanitaria locale, un comune e una regione avevano chiesto al Garante la possibilità di conservare le immagini registrate tramite un sistema di videosorveglianza per un tempo superiore alle 24 ore ma non eccedente la settimana. Al riguardo, il Garante ha evidenziato che –fatte salve le speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi o richieste investigative dell'autorità giudiziaria o di polizia giudiziaria– la conservazione deve essere limitata alle 24 ore successive alla rilevazione e solo in alcuni casi, per peculiari esigenze tecniche o per la

particolare rischiosità dell'attività svolta dal titolare del trattamento, può ritenersi ammesso un tempo più ampio, che non superi comunque la settimana.

In tale quadro, spetta al titolare del trattamento valutare la sussistenza in concreto dei presupposti che giustificano la conservazione delle immagini raccolte, per un periodo di tempo inferiore alla settimana; la conservazione delle immagini per un periodo superiore necessita invece della verifica preliminare dell'Autorità (punti 3.2.1. e 3.4. del cit. *provvedimento* generale; art. 17 del Codice) (*Note* 28 luglio; 7 dicembre; 13 dicembre e 20 dicembre 2010).

A seguito di segnalazioni e di quesiti, sono stati forniti chiarimenti anche sull'istallazione di sistemi di videosorveglianza presso istituti scolastici ribadendo, in particolare, la necessità di garantire "*il diritto dello studente alla riservatezza*" (art. 2, comma 2, d.P.R. 24 giugno 1998, n. 249) e prevedendo opportune cautele al fine di assicurare l'armonico sviluppo della personalità dei minori. L'utilizzo di sistemi di videosorveglianza è ammissibile solo se indispensabile per tutelare l'edificio ed i beni scolastici da atti vandalici, riprendendo solo le 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 extrascolastiche all'interno della scuola (punto 4.3.1.).

Inoltre, laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo le aree non strettamente pertinenti l'edificio (punto 4.3.2.); infine è stato ricordato che il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (*Note* 28 luglio e 28 dicembre 2010).

Sempre in ambito scolastico, talune rappresentanze sindacali avevano lamentato la collocazione delle telecamere in prossimità dell'apparecchiatura marcatempo utilizzata per rilevare le presenze del personale ATA o del registro utilizzato dai docenti per documentare le loro presenze, in modo da rendere possibile un controllo dell'attività dei lavoratori.

Al riguardo, è stato fatto presente che nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, e quindi di installazione di apparecchiature specificatamente preordinate alla predetta finalità; non devono perciò essere

effettuate riprese al fine di verificare la correttezza nell'esecuzione della prestazione lavorativa (ad es., orientando la telecamera sul *badge*). Inoltre, quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive ovvero è richiesta per la sicurezza del lavoro, devono essere osservate le garanzie previste in materia: in tali casi gli impianti "*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*" (artt. 4 e 8, l. 20 maggio 1970, n. 300; artt. 113 e 114 del Codice; art. 2 d.lgs. 30 marzo 2001, n. 165) (*Note* 7 e 15 dicembre 2010).

Le garanzie in materia di controlli a distanza dell'attività lavorativa sono state richiamate anche nei confronti di una Regione e di una sede territoriale della motorizzazione civile che avevano installato gli impianti di videosorveglianza presso i propri uffici (*Note* 6 settembre e 29 luglio 2010).

Infine, ad una azienda sanitaria dell'Emilia-Romagna è stato ricordato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti (quali le unità di rianimazione e reparti di isolamento) è limitato ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati e richiede tutti gli accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche nel rispetto del *provvedimento* generale del 9 novembre 2005 [doc. *web* n. 1191411] sul rispetto della dignità delle persone nelle strutture sanitarie.

Inoltre, il titolare del trattamento deve garantire che alle immagini rilevate per le predette finalità possano accedere solo i soggetti specificamente autorizzati; particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti di ricoverati) in reparti dove non sia consentito agli stessi di recarsi personalmente (quale quello di rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

In ogni caso, in applicazione del divieto di diffusione di immagini idonee a rivelare lo stato di salute di cui all'art. 22, comma 8, del Codice, non possono essere diffuse su *monitor* collocati in locali liberamente accessibili al pubblico immagini di persone malate.

Il mancato rispetto di quanto sopra oltre a rendere applicabili le sanzioni amministrative stabilite dall'art. 162, comma 2-*bis* e 2-*ter*, del Codice, può integrare la fattispecie di reato stabilita dall'art. 167, comma 2, del Codice. (cfr. punto 4.2. del cit. *Provv.* 8 aprile 2010) (*Nota* 15 dicembre 2010).

15.2. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Da accertamenti ispettivi svolti in seguito ad una segnalazione è risultato che, per finalità di sicurezza, presso un centro commerciale era stata installata una *webcam* in assenza della prescritta informativa e in violazione della pertinente disciplina di settore in tema di controlli a distanza dell'attività dei lavoratori (art. 4, comma 2, l. n. 300/1970), con conseguente illiceità del trattamento svolto (artt. 11, comma 1, lett. *a*) e 114, del Codice).

Il Garante ha quindi disposto il blocco del trattamento effettuato a mezzo della *webcam* installata, in attesa dell'eventuale espletamento delle procedure previste dal richiamato art. 4, comma 2, l. n. 300/1970 (*Provv.* 10 giugno 2010 [doc. *web* n. 1736167]).

L'Autorità si è poi pronunciata in relazione ad una istanza di verifica preliminare presentata da una società operante nel settore della progettazione e produzione di *smart card* principalmente per il mercato *GSM* e bancario e volta ad ampliare, quale misura di protezione ulteriore a garanzia dei clienti, i tempi di conservazione delle immagini registrate a mezzo dell'impianto di videosorveglianza installato presso la sede operativa della società; ciò, muovendo dall'assunto che l'attività svolta, assimilabile a quella della Zecca di Stato, sarebbe stata potenzialmente soggetta ad un alto rischio di illecito.

Il periodo di conservazione suggerito dalla società (90 giorni), "imposto" dagli enti certificatori (tra i più noti, VISA, MASTERCARD, *GSM Association*) anche ai fini di un eventuale rinnovo delle stesse certificazioni, avrebbe inoltre risposto all'esigenza di rafforzare le misure di prevenzione e contrasto contro possibili comportamenti fraudolenti da parte di terzi (in particolare, i lavoratori della società), consentendo l'accertamento a posteriori

di possibili illeciti di natura penale suscettibili di verifica solo a distanza di tempo dalla loro commissione (anche in ragione delle complesse procedure organizzative e produttive in essere presso la società).

L'Autorità ha rigettato l'istanza ritenendo sproporzionati i tempi di conservazione proposti in relazione alle esigenze prospettate, peraltro non sufficientemente documentate (*Provv.* 4 novembre 2010 [doc. *web* n. 1767759]). Da un lato, infatti, le "prescrizioni" impartite dagli enti certificatori sono risultate "derogabili" in presenza di "restrizioni legali" all'utilizzo di sistemi di videosorveglianza; dall'altro, non sono stati addotti elementi rigorosi tali da giustificare il segnalato allungamento dei tempi di conservazione delle immagini in rapporto alle (ipotetiche) condotte criminose descritte dalla società, peraltro mai verificatesi in concreto (verosimilmente anche in ragione delle altre numerose misure di sicurezza già approntate: accessi controllati; sensori di allarme e di movimento; sistemi di criptazione dei dati; divieto di utilizzo di strumenti di archiviazione, ecc.).

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 incidenti sull'integrità del patrimonio aziendale.

15.3. BIOMETRIA

Biometria e luoghi di lavoro

Nel corso dell'anno il Garante è stato nuovamente interpellato in ordine all'utilizzabilità, da parte di soggetti pubblici, di sistemi di rilevazione automatica per il controllo degli accessi al luogo di lavoro mediante il riconoscimento dei dati biometrici dei dipendenti. Si è reso, quindi, necessario ribadire le indicazioni contenute nel *provvedimento* generale recante le linee-guida in materia (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In particolare, il Garante ha ricordato ad una amministrazione comunale, a seguito di una specifica segnalazione di un sindacato che, di regola, i sistemi di rilevazione di impronte digitali possono essere attivati soltanto per l'accesso a speciali aree dei luoghi di

lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza, in relazione a particolari necessità e nel rispetto di specifiche condizioni indicate nel cit. *provvedimento* generale (cfr. punto 7.2.). Il Comune è stato quindi invitato a verificare l'eventuale sussistenza di tali condizioni e ad informare l'Ufficio in ordine alle misure volte ad assicurare il rispetto di quanto indicato (*Nota* 20 dicembre 2010; v., *infra*, *Nota* 31 dicembre 2010).

In un'altra occasione, in risposta alle preoccupazioni manifestate da un Prefetto, circa istanze sindacali relative al trattamento di dati biometrici dei lavoratori italiani presso una base militare degli Stati Uniti, il Garante, con disponibilità ad esaminare eventuali profili critici, ha ricordato che, nel corso di una fruttuosa attività di collaborazione con l'Ambasciata americana, sono state fornite puntuali indicazioni anche sugli adempimenti procedurali necessari per rendere il trattamento conforme alla disciplina sulla protezione dei dati. Da ultimo l'Ambasciata si era riservata di valutare la possibilità di formulare all'Autorità una richiesta di interpello per l'implementazione di una carta elettronica che consenta l'accesso ai sistemi informatici delle basi militari (*Nota* 9 luglio 2010).

Nel fornire indicazioni ad alcuni dipendenti italiani di un'altra base militare americana, l'Ufficio ha precisato che il trattamento dei dati biometrici effettuato per le sole finalità di autenticazione informatica non richiede la valutazione preventiva del Garante. L'adozione di un sistema di autenticazione informatica (conforme ai requisiti tecnici indicati dalle regole 1-11 dell'Allegato B. al Codice) costituisce infatti una misura minima di sicurezza, che deve essere adottata ai sensi dell'art. 34, comma 1, lett. *a*), del Codice. Tali credenziali di autenticazione possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave (*Nota* 31 dicembre 2010).

Con riferimento all'uso delle impronte digitali dei lavoratori per l'accesso a particolari aree riservate sono state richiamate le regole restrittive di cui sopra si è fatto cenno, indicate nel *provvedimento* 14 giugno 2007 [doc. *web* n. 1417809], in particolare al punto 7.2. (*Nota* 31 dicembre 2010; v., *supra*, *Nota* 20 dicembre 2010).

Pur rientrando tra le legittime facoltà del datore di lavoro quella di sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 c.c.), verificando le presenze dei

dipendenti e il rispetto dell'orario di lavoro, le imprese che intendono adottare sistemi di lettura delle impronte digitali per verificare la presenza in servizio dei dipendenti devono prima dimostrare che le finalità di controllo non possano essere realizzate con sistemi meno invasivi, nel rispetto dei princìpi di necessità e di proporzionalità.

Con questa motivazione l'Autorità ha respinto le richieste di verifica preliminare, ai sensi dell'art. 17 del Codice, con le quali due società di trasporti chiedevano di poter usare, presso le proprie aziende, un meccanismo di autenticazione biometrico (*provvedimenti* 17 novembre 2010 [doc. *web* nn. 1779745 e 1779758]).

Secondo le società, il rilevamento delle impronte avrebbe potuto evitare eventuali condotte irregolari, come lo scambio di *badge* attestanti la presenza in servizio, con conseguenti maggiori garanzie per l'incolumità degli utenti e del personale viaggiante. Nel corso dell'istruttoria, tuttavia, è emerso che i tradizionali metodi di controllo si erano dimostrati più che sufficienti a garantire la verifica della presenza in servizio dei dipendenti.

L'uso dei sistemi biometrici era stato richiesto dalle due società anche per accedere ai locali nei quali venivano custodite le banche dati cartacee e informatiche contenenti i dati personali dei dipendenti. Dagli accertamenti effettuati dal Garante è invece emerso che tali dati, lungi dall'essere caratterizzati da specifiche peculiarità, non richiedevano particolari sistemi di controllo, trattandosi di informazioni solitamente elaborate dagli uffici amministrativi di qualsiasi azienda.

16. Il Registro dei trattamenti

In attuazione della direttiva europea relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Direttiva n. 95/46/CE), in riferimento alla quale la Commissione europea ha pubblicato il 4 novembre 2010 una Comunicazione che fissa le linee generali per la revisione di tale direttiva aprendo una consultazione pubblica conclusasi il 15 gennaio 2011, il Codice prevede che l'Autorità abbia il compito di tenere il Registro dei trattamenti, formato sulla base delle notificazioni ricevute (così l'art. 154, comma 1, lett. *l*), del Codice).

Tale Registro, secondo quanto disposto dall'art. 37, comma 4, del Codice deve essere accessibile a chiunque e consultabile gratuitamente per via telematica.

Tali condizioni di accessibilità sono state garantite fin dal 2004, con la realizzazione di una procedura di notificazione telematica ed un'apposita sezione del sito Internet dell'Autorità, dedicata alla consultazione *online* del Registro.

La notificazione consiste in una dichiarazione formale compilata direttamente sul *computer* dell'utente, con la quale vengono comunicati al Garante i trattamenti di dati suscettibili di recare particolare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali. (cfr. artt. 37 e 38 del Codice; *Provv.* 31 marzo 2004 [doc. *web* n. 852561]; *Relazione* 2004, p. 109 ss.).

Con riguardo, in particolare, alle modalità di compilazione del modello informatico e ai suoi contenuti, il Garante, che sin dal 2004 ha introdotto profondi cambiamenti in relazione ai profili procedurali della notificazione, ha operato una ulteriore semplificazione con il *provvedimento* a carattere generale del 22 ottobre 2008 [doc. *web* n. 1571196] nel contesto di modifiche normative volte alla semplificazione ed all'accelerazione delle procedure amministrative.

Tale *provvedimento*, in particolare, ha individuato il nuovo modello di notificazione e, tra l'altro, ha limitato i casi in cui si deve indicare il luogo principale di custodia dei dati ed ha sottratto al pagamento dei diritti di segreteria la modifica di elementi quali il numero telefonico, di fax e l'indirizzo di posta elettronica del titolare.

Il servizio di assistenza ai titolari notificanti ed agli utenti del Registro si è avvalso ulteriormente, nel corso del 2010, degli strumenti di messaggistica elettronica. I rapporti con il notificante sono infatti gestiti sia tramite messaggi originati in automatico dalla procedura telematica di notificazione, sia attraverso e-mail predisposte in modo specifico dal personale addetto, pur rimanendo sempre attivo il servizio di supporto telefonico. L'utilizzazione sempre più ampia di tali strumenti, grazie anche alla maggiore confidenza del pubblico con gli stessi, ha consentito una più efficiente e rapida risposta dell'Autorità alle esigenze dell'utenza.

Sempre maggiore è il numero dei cittadini che si sono avvalsi del servizio di assistenza garantito dal dipartimento. Si mantengono inoltre costanti gli accessi diretti al Registro da parte degli utenti, con una media giornaliera vicina ai 90 accessi e punte superiori ai 300. La verifica senza intermediazioni delle notificazioni segna la piena realizzazione del dettato dell'art. 37, comma 4, del Codice sulla consultazione telematica gratuita del registro. A ciò hanno contributo in modo determinante la possibilità sia di seguire l'*iter* delle diverse modifiche e cessazione successive alla prima notificazione, anche in caso di cambiamento totale della denominazione del titolare, sia di fruire direttamente delle funzioni di stampa integrale delle notificazioni, nonché le modalità di ricerca particolarmente efficienti e di facile utilizzazione.

Le tradizionali attività di controllo delle notificazioni inserite nel Registro e di accertamento delle violazioni dell'obbligo di notificazione sono state intensificate, anche grazie al rapporto sinergico con le attività ispettive del Garante.

Il 2010 ha fatto registrare la ripresa del numero di notificazioni presentate (come negli anni precedenti tale dato è fornito su base annuale), con una inversione di tendenza rispetto al dato registrato nel 2009. Con circa il 14% in più rispetto all'anno precedente, vi è stato infatti il sostanziale recupero dei livelli del 2008.

Per quanto concerne il complesso delle notificazioni presenti nel Registro (il periodo di riferimento è infatti quello 2004-2010), i dati percentuali relativi alla tipologia dei trattamenti notificati, rimangono sostanzialmente inalterati. I trattamenti volti a definire il profilo e la personalità dell'interessato tramite l'ausilio di strumenti elettronici (27%), i

trattamento 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 (20%), coprono da soli quasi il 70% di tutti i trattamenti notificati.

È opportuno segnalare solo un lieve aumento dei trattamenti che utilizzano dati sensibili a fini di selezione del personale conto terzi che passano dal 5% al 6%.

In merito infine alla distribuzione geografica dei titolari, vale quanto già evidenziato negli anni precedenti. Il nord del Paese rappresenta da solo il 57% dei notificanti. Tale decisa prevalenza potrebbe essere ascrivibile tanto a diversità economiche di natura strutturale quanto ad una più decisa incidenza della crisi economica sulla tipologia dei titolari con sede nel meridione (ditte individuali, artigiani, società a responsabilità limitata di piccole o piccolissime dimensioni).

Con riguardo all'ambito europeo si segnala, per completezza che, in vista della revisione della Direttiva n. 95/46/CE, il Gruppo Art. 29 ha redatto una lettera, inviata alla Commissione europea, con allegato anche un *paper* in materia di notificazione in cui vengono illustrate le diverse opzioni proposte e le soluzioni che hanno ottenuto la maggioranza dei consensi da parte dei vari Paesi (in particolare, si propende per un sistema basato su una "lista positiva secondo il modello italiano"). Sul punto si rinvia al paragrafo 20.2. della *Relazione*.

17. LA TRATTAZIONE DEI RICORSI

17.1. CONSIDERAZIONI GENERALI

La lettura dei dati statistici riferiti all'anno appena trascorso permette di sistematizzare attorno ad alcuni punti fermi la congerie di informazioni che, anche per l'ampiezza dei temi trattati, ruota intorno ai molti ricorsi sottoposti all'esame dell'Autorità ed induce a considerazioni di carattere generale. Volendo trovare un termine sintetico che esprima e riassuma il lavoro in materia svolto nel 2010 si può forse parlare di "assestamento", in senso sia quantitativo, sia "contenutistico". Il primo dato che emerge è infatti il totale di ricorsi formali (proposti cioè nel rispetto dei requisiti di cui all'art. 145 ss. del Codice) decisi dall'Autorità nell'anno solare 2010: 349. È un numero praticamente uguale a quello registrato nell'anno precedente e che conferma un *trend* recente, di sostanziale stabilizzazione di queste cifre, che sono però sicuramente più basse di quelle registrate nei primi anni del nuovo secolo. Comprendere le ragioni di questa diminuzione e valutare se lo strumento del ricorso possa avere potenzialità non ancora espresse non è facile. Alcune considerazioni di carattere generale sono però proponibili. Anzitutto si può riconoscere e verificare in termini positivi l'effetto deflattivo sul contenzioso apportato dai provvedimenti di carattere generale adottati dal Garante (fenomeno che trova evidenza anche nelle decisioni adottate a seguito della presentazione di segnalazioni e reclami). A cominciare dall'entrata in vigore del codice di deontologia concernente i trattamenti di dati da parte delle *cd.* "*centrali rischi private*" (inizi 2005), l'azione del Garante ha visto una nutrita elaborazione di molteplici provvedimenti generali, quali le linee-guida, e appunto i codici di deontologia, che, spesso anche in chiave preventiva, hanno chiarito e indirizzato il trattamento dei dati personali in diversi settori della vita economica e sociale. Molti provvedimenti generali sono stati elaborati proprio per risolvere i vari dubbi operativi che i diversi interessati (anche attraverso il contenzioso) avevano portato all'attenzione dell'Autorità.

Da questo punto di vista, molti ricorsi che ora pervengono sono una spia di fenomeni che meritano attenta considerazione. Da una parte, registrano le inevitabili lacune proprie di qualsiasi sistematizzazione normativa o paranormativa ed impegnano il Garante ad una

continua revisione e ad un costante aggiornamento delle sue decisioni (ivi compresi i codici di deontologia già adottati), dall'altra indicano nuove frontiere per l'attività dell'Autorità nei prossimi anni. Da un lato possiamo, a titolo di esempio, citare i non numerosi casi di difficoltà interpretative nella disciplina sui sistemi di informazioni creditizie. Dall'altro, i sempre più numerosi procedimenti che coinvolgono la riflessione sul trattamento dati nei *cd.* "*social network*".

Volendo poi ipotizzare altre ragioni dell'assestamento quantitativo dei ricorsi, si può fare riferimento alla moltiplicazione, nei più diversi campi applicativi, di procedimenti di mediazione e composizione delle liti, con i quali è possibile attivare forme di tutela ugualmente rapide e tendenzialmente specializzate, ottenendo la tutela di posizioni sostanziali (ad es., corretta gestione di un rapporto contrattuale) rispetto alle quali, spesso, l'esercizio dei diritti previsto dalla disciplina in materia di protezione dei dati personali ha un ruolo strumentale e preparatorio. Emblematico al riguardo è il campo dei rapporti concernenti la fornitura di servizi telefonici e telematici, rispetto ai quali si è fortemente sviluppata negli ultimi anni l'azione dei comitati regionali per le comunicazioni (CORECOM). In questo quadro merita attenzione, nei prossimi mesi, il primo dispiegarsi della procedura di mediazione civile obbligatoria prevista dal d.lgs. 4 marzo 2010, n. 28. Tutte le materie nelle quali opererà la nuova procedura comportano infatti un ampio trattamento di dati personali.

Non va poi dimenticato che la tutela innanzi al Garante con lo strumento del ricorso è alternativa a quella giurisdizionale dinanzi al giudice ordinario, nelle forme e nei modi di cui all'art. 152 del Codice. Da questo punto di vista gli ultimi anni hanno visto sicuramente crescere l'utilizzo della via giudiziaria "tradizionale" non solo per la tutela dei diritti previsti dal Codice, ma anche per i profili di tipo risarcitorio che ad essa logicamente si connettono (e rispetto ai quali il Garante non ha competenza).

17.2. DIRITTI ESERCITATI, TIPOLOGIA DEI RICORSI, TIPI DI DECISIONI ADOTTATE

Riflettere sulla pluralità e varietà di posizioni giuridiche che possono essere tutelate sulla base dell'art. 7 del Codice induce a chiedersi quali siano i diritti più frequentemente esercitati con lo strumento del ricorso. Sotto un "cappello" normativo unico ricadono

infatti sia diritti mirati ad aumentare, dettagliare o integrare il patrimonio conoscitivo dell'interessato (conoscere i dati, aggiornarli, definire le figure del titolare o del responsabile del trattamento, avere contezza dell'ambito di circolazione delle informazioni stesse, ecc.) sia diritti volti a contrastare l'utilizzo che altri faccia di quelle medesime informazioni (vanno in questo senso, ad esempio, la richiesta di cancellare dati trattati in violazione di legge o di opporsi per motivi legittimi al loro ulteriore trattamento). Di fatto, la stragrande maggioranza dei ricorsi è incentrata su tre tipologie di esercizio dei diritti di cui al cit. art. 7, a volte compresenti nella medesima vicenda: 1) la richiesta di accesso ai dati personali (facendo leva sull'estrema latitudine di questo diritto che conosce pochissime zone franche e limitate ipotesi di differimento del suo esercizio); 2) l'opposizione a trattamenti di dati indesiderati (valvola di sfogo essenziale, ad esempio, contro tutte le forme di attività promozionali più o meno invasive); 3) le richieste di cancellazione di dati di cui si assume l'illecita acquisizione o l'illecito utilizzo.

Considerazioni interessanti possono essere tratte anche dall'esame delle principali tipologie di titolari di trattamento, nei confronti dei quali quei diritti sono fatti valere. In proposito, a conferma di un *trend* ormai consolidato, l'ambito che ha registrato anche nell'anno 2010 il maggior numero di ricorsi è quello bancario-finanziario in genere. In questo settore si cumulano i procedimenti relativi all'accesso ai dati detenuti da istituti di credito e da società finanziarie con i ricorsi rivolti più specificamente a porre in discussione particolari trattamenti connessi all'esecuzione dei contratti di settore.

Il filo conduttore è peraltro quasi sempre relativo alle situazioni di contenzioso, di crisi o di difficoltà dei risparmiatori o delle imprese. In questo contesto il ricorso è spesso strumento necessario per acquisire le informazioni utili a contestare una non corretta gestione di risparmi, per verificare la liceità delle condizioni di un finanziamento, per controllare il corretto flusso dei dati fra un ente finanziatore e gli archivi di un sistema di informazioni creditizie, così come per verificare i dati di un'impresa forniti da un soggetto operante nel settore delle *cd.* "*informazioni commerciali*".

A questo filone principale si avvicinano, per numero di ricorsi proposti, i procedimenti concernenti il trattamento dei dati nell'ambito del rapporto di lavoro e quelli concernenti

l'opposizione alle più diverse forme di utilizzo dei dati per l'invio di comunicazioni promozionali indesiderate.

Infine merita qualche breve notazione anche il tipo di decisioni che vengono adottate all'esito dei procedimenti di ricorso.

Da questa prospettiva si nota, nell'ultimo anno, il significativo aumento delle decisioni di accoglimento (in tutto o in parte) delle richieste avanzate dagli interessati. È un indice che rimanda sicuramente all'uso sempre più mirato ed affinato di questo strumento di tutela. Resta comunque preponderante la quantità di casi conclusi con una declaratoria di non luogo a provvedere. È questo (al di là del *nomen iuris* che può ingannare) un segno di efficacia dello strumento di tutela e la prova della possibilità di ripristinare con esso la tutela effettiva dei diritti violati (ovviamente nello specifico raggio d'azione perimetrato dall'art. 7 del Codice). Ciò è in particolare vero per l'esercizio del diritto di accesso e per l'opposizione al trattamento per fini promozionali poiché spesso, a fronte del silenzio serbato al momento della ricezione dell'interpello preventivo, il titolare del trattamento, al momento della presentazione del ricorso, provvede celermente alla tutela dei diritti violati favorendo così una veloce definizione del procedimento.

Resta ancora relativamente elevato il numero di procedimenti che si concludono con declaratorie di inammissibilità, segno di un utilizzo non sempre corretto del procedimento *ex* art. 145 ss. del Codice. In particolare questo è l'indice del tentativo di utilizzare uno strumento indubbiamente agile e semplice per la tutela di posizioni giuridiche sostanziali non comprese tra i diritti precisamente enumerati nell'art. 7 del Codice, o per ottenere il riconoscimento di profili (ad es., quelli risarcitori), per i quali la tutela può essere invocata solo dinanzi all'autorità giudiziaria ordinaria.

17.3. PROFILI PROCEDURALI

L'esame particolareggiato della casistica mette in luce alcuni aspetti procedurali, che meritano di essere ricordati al fine di prevenire il rischio di declaratorie di inammissibilità. La procedura dei ricorsi è sicuramente abbastanza semplice e priva di eccessive formalità. Ciò non toglie che alcuni "paletti" minimi sono considerati nell'art. 145 ss. del Codice.

Va anzitutto ricordato che l'atto di ricorso può essere proposto solo dopo che siano integralmente trascorsi 15 giorni dalla ricezione (da parte del titolare del trattamento) dell'interpello preventivo con il quale siano stati chiaramente esercitati i diritti di cui all'art. 7 del Codice. La presentazione diretta del ricorso è infatti possibile solo qualora sia realmente presente (e documentabile) un pregiudizio "imminente e irreparabile", che potrebbe derivare all'interessato dal decorso del pur breve lasso di tempo di 15 giorni di cui si è detto. Si tratta di ipotesi del tutto eccezionale, oggetto di attento vaglio da parte del Garante. Quando non è dato rinvenirla e la presentazione diretta del ricorso appare un aggiramento di una disposizione molto specifica, il Garante emana, inevitabilmente, delle decisioni di inammissibilità (*Provv.* 21 ottobre 2010 [doc. *web* n. 17682206]). Parimenti inequivoca deve essere l'identificazione del titolare del trattamento, fin dalla fase iniziale dell'esercizio dei diritti di cui all'art. 7. Non è pertanto possibile porre a base di un ricorso istanze del tutto generiche, spesso contenenti richieste che esulano dal campo di applicazione della legge sulla protezione dei dati personali, così come non si possono ritenere valide note inviate al titolare per mera conoscenza (*Provv.* 23 settembre 2010 [doc. *web* n. 1761903]).

Problemi a volte più delicati nascono in relazione all'esercizio del diritto di accesso. È infatti ancora non sempre compresa la distinzione fra esercizio del diritto di accesso ai dati personali (cui è specificamente rivolta l'attenzione del Garante) e richieste di accesso ad atti amministrativi o a copie di documenti detenuti anche da soggetti privati (banche, assicurazioni, ecc.). Quella che può sembrare una mera questione nominalistica è invece questione di sostanza che rimanda all'esatto confine delle diverse normative e comporta rilevanti differenze in ordine al raggio d'azione dei distinti diritti esercitati (basti pensare ai profili relativi all'acquisizione di informazioni riferite a terze persone).

17.4. LA CASISTICA PIÙ SIGNIFICATIVA

In questa sezione vengono esaminati solo alcuni dei settori che sono stati interessati dalla presentazione di ricorsi. Sono comunque sufficienti per dare un'idea della varietà di situazioni interessate da questa particolare forma di contenzioso e per mettere in luce alcuni ambiti di trattamento di particolare interesse.

17.4.1. Rapporto di lavoro

L'importanza dei profili di protezione dei dati in questo ambito è andata crescendo negli ultimi anni. Il fenomeno è strettamente connesso alla moltiplicazione dei tipi di informazioni riferite ai prestatori di lavoro che sono oggetto di comune trattamento nelle più varie realtà lavorative. È infatti ormai di amplissima diffusione la raccolta di informazioni relative a giudizi e valutazioni delle prestazioni professionali, così come sempre più articolata e complessa è la procedura che porta alla definizione di questi giudizi (cui è spesso legata una aliquota significativa della retribuzione o da cui dipendono le progressioni di carriera dei dipendenti).

Sotto un altro punto di vista, le modalità di svolgimento delle prestazioni lavorative nell'attuale società tecnologica determinano, e in molti casi addirittura impongono, un utilizzo massivo di dati e informazioni personali connessi all'utilizzo dei *computer* o comunque relativi all'impiego della rete Internet. Non stupisce che su questi terreni si sia sviluppata in tempi brevi una rilevante casistica. Vanno così brevemente ricordate alcune decisioni significative. Dall'accoglimento della richiesta di una dipendente di un ospedale ad accedere alle informazioni contenute nel foglio presenze e nelle relazioni predisposte dalle responsabili del reparto presso il quale prestava servizio (*Provv.* 29 settembre 2010 [doc. *web* n. 1765061]) alla vicenda di un impiegato licenziato che ha chiesto al Garante di accedere nella sua completezza al proprio fascicolo personale, comprensivo delle valutazioni annuali e delle schede di *job description* che lo riguardavano (richiesta accolta con *Provv.* 17 novembre 2010 [doc. *web* n. 1778268]). Così come la richiesta di accesso ai dati può essere lo strumento per ricostruire anche lunghi periodi lavorativi (ottenendo la specificazione degli orari dei turni di servizio e dei luoghi di svolgimento delle prestazioni lavorative, come nel *Provv.* 22 aprile 2010 [doc. *web* n. 1724445]).

Ma le problematiche senza dubbio più significative sono emerse da una prima, significativa serie di provvedimenti che hanno portato all'esame dell'Autorità ipotesi di trattamento di dati svolti a seguito di controllo sul corretto uso, da parte di dipendenti, degli strumenti di lavoro aziendali di tipo informatico. Sono tutte vicende nelle quali il ricorso si è inserito in un contenzioso già aperto, e in diversi casi già caratterizzato dall'avvenuto

licenziamento del prestatore di lavoro. Le fattispecie di partenza sono state sostanzialmente analoghe pur in uno spettro ampio di ipotesi: dalla contestazione relativa all'aver "scaricato dalla rete Internet", sul *computer* aziendale in dotazione, *software* per la condivisione di *file*, alla verifica dell'esistenza sul disco fisso del *computer* di *file* di contenuto pornografico o comunque estranei all'attività lavorativa, all'utilizzo, a fini di contestazione disciplinare, di informazioni desunte da scambi di e-mail tramite l'utenza aziendale fino all'ipotesi dell'utilizzo del telefono cellulare aziendale in dotazione per intrattenere contatti e relazioni con una società concorrente. Nel decidere questi casi il Garante ha tenuto una linea di valutazione costante che può riassumersi intorno ad alcuni capisaldi:

1) il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro;
2) nel far questo, però, occorre rispettare la libertà e la dignità dei lavoratori nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i princìpi di correttezza, di pertinenza e di non eccedenza di cui all'art. 11 del Codice. Ciò tenuto anche conto del fatto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile;
3) in concreto, il Garante ha sempre verificato, nei casi sottoposti alla sua attenzione, se il ricorrente era stato previamente informato circa gli eventuali controlli che il datore di lavoro poteva effettuare sugli strumenti informatici, nonché sulle modalità da seguire per gli stessi (ad es., circa la presenza dell'interessato, di rappresentanti sindacali, di personale all'uopo incaricato). Su questa tematica si possono vedere fra le altre le decisioni del 1° aprile 2010 [doc. *web* n. 1717799]; 10 giugno 2010 [doc. *web* n. 1736780]; 13 gennaio 2011 [doc. *web* n. 1792605].

17.4.2 Trattamento di dati in ambito giornalistico

Anche l'esame delle vicende concernenti il trattamento di dati personali in ambito giornalistico mette in luce gli effetti che su una fattispecie-base di tipo tradizionale (in questo caso generalmente la liceità o meno della raccolta e della diffusione di dati e

informazioni) produce l'attuale pervasivo dispiegarsi delle nuove tecnologie. È infatti facile notare come ormai gran parte delle vicende in ambito giornalistico portate all'attenzione del Garante concernono, più che i profili strettamente connessi alla verità e correttezza delle informazioni fornite, le modalità con le quali tali informazioni sono rese disponibili sulla rete Internet attraverso i siti delle testate giornalistiche (v., ad es., *Provv.* 1° luglio 2010 [doc. *web* n. 1746519]) o, in altri casi, le forme e i modi (sempre più pervasivi) con i quali molti dati vengono "captati" e fatti oggetto di cronaca giornalistica. Il catalogo degli esempi è molto vasto: dalle più recenti frontiere del giornalismo d'inchiesta che utilizza spesso microtelecamere nascoste per documentare fatti altrimenti difficilmente proponibili all'attenzione della pubblica opinione, alla presenza dilagante di dati trattati dai *social network*, all'acquisizione e al "rilancio" in chiave di cronaca giornalistica di scambi di opinione all'interno di *forum* e *blog*, alla divulgazione del contenuto di messaggi *Sms*, fino alle ben note problematiche legate all'uso di materiali d'indagine depositati agli atti di procedimenti penali, fra cui le spesso copiose intercettazioni telefoniche messe sempre più frequentemente a disposizione anche nel formato audio (*Provv.* 13 maggio 2010 [doc. *web* n. 1735420] e *Provv.* 3 febbraio 2011 [doc. *web* n. 1793828]).

L'impressione generale è che la potenza dei nuovi mezzi sfugga alla capacità di governo dei vari attori, con una tendenza (cui anche l'Autorità non può sottrarsi) a "inseguire", con gli strumenti tradizionali del diritto congiunti (auspicabilmente) al buon senso operativo, una casistica sempre più eterogenea.

Dimostrazione emblematica di questa realtà è la problematica connessa alla messa a disposizione *online* libera e gratuita degli archivi storici dei quotidiani. La disponibilità sulla rete di questa enorme massa di informazioni (unita alla capacità di collegamento e di "*aggregazione informatica*" dei *cd.* "*motori di ricerca*") ha portato ad emersione i problemi connessi alla associazione di notizie ormai datate, in tanti casi contenenti riferimenti "negativi" (per quanto originariamente esatti) a persone comuni che vedono ora "rilanciati" in rete episodi legati a fasi ormai lontane della propria esperienza di vita. Il problema, estremamente serio, coinvolge diritti e interessi di sicuro rilievo anche costituzionale il cui bilanciamento si dimostra spesso problematico. Non è facile infatti equilibrare, da

un lato, le iniziali finalità giornalistiche con le attuali finalità documentaristiche che legittimano l'ulteriore conservazione per fini storici, e, dall'altro, le esigenze di tutela di persone che possono legittimamente invocare, in certi casi e a determinate condizioni, l'oblio su vicende ormai non più attuali e lontane (anzi spesso confliggenti) con il proprio attuale percorso di vita. Ciò tenendo conto che le enunciate finalità di tipo storico postulano naturalmente una conservazione "integrale" della memoria del passato, che mal si concilia con le aspirazioni di molti interessati ad ottenere cancellazioni, aggiornamenti e modificazioni dei dati. Il tema sta interessando l'Autorità da almeno due anni e di esso è stata data evidenza anche nella scorsa *Relazione* (p. 9 ss.). Nel 2010 l'orientamento del Garante non è cambiato ed il punto di equilibrio fra le contrapposte esigenze è stato trovato nel ricorso ai protocolli informatici che permettono (nei casi che il Garante ha ritenuto meritevoli di protezione) di interdire l'indicizzazione automatica, da parte dei motori di ricerca esterni ai siti Internet dove le pubblicazioni *online* vengono riproposte, delle pagine o delle sezioni contenenti dati personali che per il lungo tempo trascorso, la natura non pubblica del soggetto interessato, la lesività che l'informazione può comportare, la mancanza di interesse attuale alla diffusione giornalistica del dato, non sia più opportuno che vengano fatte oggetto di indicizzazione e quindi di disponibilità indiscriminata sulla rete Internet. Ciò, ferma restando la conservazione integrale dei medesimi "pezzi" giornalistici sul sito Internet "sorgente", in modo da permettere comunque uno sguardo integrale su pubblicazioni storicamente avvenute e quindi non sottraibili alle esigenze della conservazione e dell'utilizzo a fini di ricerca storica e scientifica (v., sul punto, fra gli altri, provvedimenti 3 giugno 2010 [doc. *web* n. 1734459] e 15 luglio 2010 [doc. *web* n. 1746654]).

17.4.3. Trattamento di dati in ambito bancario e informazioni commerciali

Si è già fatto cenno al gran numero di ricorsi che hanno riguardato l'ambito bancario-finanziario complessivamente inteso. L'elevato numero dei procedimenti e la tipologia delle richieste avanzate (fondamentalmente volte ad acquisire cognizione di informazioni utili a ricostruire il quadro dei rapporti intrattenuti con gli istituti di credito o a sollecitare

la cancellazione di evidenze negative associate a determinati interessati) si pongono in sostanziale continuità con le esperienze degli anni più recenti. Si è ormai delineato un utilizzo degli strumenti di tutela messi a disposizione dall'art. 7 del Codice finalizzato, alternativamente o in connessione con altri mezzi quali quelli previsti dal testo unico bancario, ad acquisire informazioni volte essenzialmente a: a) ricostruire posizioni contabili di persone defunte da parte di soggetti interessati alla corretta allocazione dell'asse ereditario; b) raccogliere tutti i dati relativi a contratti di investimento o ad altre posizioni bancarie al fine (spesso) di contestare i tassi di interesse o la regolarità dei rapporti medesimi, o per verificare la sussistenza e la validità delle informazioni ricevute e dei consensi prestati.

A fianco di queste ipotesi si collocano poi le richieste di cancellazione dei dati di tipo "negativo" che, su indicazione delle banche, vengono riportate, a seconda dei contesti, negli archivi dei sistemi di informazioni creditizie, nella Centrale dei rischi della Banca d'Italia o nell'archivio elettronico della Centrale d'allarme interbancaria. Si tratta di materia che trova regole (anche procedurali) dettagliate nelle relative discipline di settore o nell'apposito codice di deontologia concernente il settore del *cd.* "*credito al consumo*". Ed è proprio alla verifica del rispetto di questa normativa che rimandano i provvedimenti in merito del Garante (v., fra tanti, *Provv.* 27 aprile 2010 [doc. *web* n. 1733190]; *Provv.* 22 luglio 2010 [doc. *web* n. 1748844]).

In qualche modo connesso a questa problematica è il trattamento di dati ricavati dal Registro delle imprese, dagli archivi delle ex conservatorie dei registri immobiliari o da altre fonti pubbliche e relativi, ad esempio, ai soggetti titolari di quote azionarie o di cariche sociali, ai dati sugli eventuali fallimenti o su altre vicende economicamente e giuridicamente rilevanti per la vita delle imprese. Tali informazioni sono fatte oggetto di aggregazione, valutazione e commento, in modo generalmente informatizzato, da parte dei soggetti che operano nel settore delle *cd.* "*informazioni commerciali*". La rilevanza di questa attività e la potenziale risonanza negativa che questo tipo di informazioni può avere sulla reputazione economica di molti imprenditori ha determinato negli ultimi anni un cospicuo contenzioso in materia. La necessità di affrontare organicamente la materia e di

fissare "paletti" condivisi nel trattamento di queste informazioni ha spinto l'Autorità a promuovere l'apertura dei lavori mirati alla sottoscrizione di un codice di deontologia *ad hoc* per questo settore, cui già il d.lgs. n. 196/2003 faceva peraltro riferimento all'art. 118. I lavori per la redazione del codice sono stati avviati all'inizio del 2011 e procedono con l'attiva collaborazione sia dei soggetti rappresentativi degli operatori economici del settore, sia di soggetti portatori di interessi qualificati in relazione alla tipologia di dati trattati (ad es., banche ed associazioni di consumatori e utenti).

18. Il contenzioso giurisdizionale

18.1. Considerazioni generali

Anche nel 2010 è stata confermata l'importanza del ricorso previsto dall'art. 152 del Codice, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante.

A fronte dei 146 ricorsi del 2009, sono stati trattati dall'Autorità 135 ricorsi relativi a giudizi proposti nel 2010 non coinvolgenti direttamente pronunce del Garante.

Atteso l'elevato numero di tali controversie, assumono sempre maggiore rilevanza l'obbligo di notifica al Garante di tutti i ricorsi presentati all'autorità giudiziaria (art. 152, comma 7) e 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).

Tali strumenti consentono al Garante di avere un'ampia informazione sull'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere la funzione di segnalazione al Parlamento e al Governo degli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

18.2. Profili procedurali

Il procedimento introdotto dall'art. 152 prevede che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento (comma 2).

In tema di giurisdizione, analogamente a quanto accaduto nel 2009, nel corso del 2010 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.

In tema di competenza territoriale si è appreso che il Tribunale di Perugia, sezione distaccata di Todi, in applicazione del disposto di cui all'art. 152, comma 2, del Codice, ha dichiarato la propria incompetenza territoriale a conoscere della controversia ivi azionata in favore del tribunale del luogo dove risiede il titolare del trattamento ovvero, nel caso di specie, il Tribunale di Roma (sentenza n. 15 del 19 febbraio 2008).

18.3. PROFILI DI MERITO

Analogamente a quanto verificatosi nello scorso anno, su alcune pronunce emesse dall'Autorità giudiziaria, relative a fattispecie in cui non erano in discussione provvedimenti adottati dal Garante, ha trovato applicazione l'art. 137 del Codice in tema di bilanciamento tra l'esercizio del diritto di cronaca e il diritto alla tutela dei dati personali, confermando che si tratta di un tema che frequentemente genera contenzioso.

In particolare 7 decisioni hanno accertato la violazione del corretto esercizio del diritto di cronaca relativamente al mancato rispetto del principio dell'essenzialità dell'informazione, con specifico riferimento alla pubblicazione di dati personali, idonei a identificare i protagonisti di alcuni fatti di cronaca o a rivelare aspetti intimi della loro vita, ritenuti non indispensabili al soddisfacimento dell'interesse pubblico alla conoscenza delle vicende descritte.

In tal senso si è pronunciato il Tribunale di Milano che, in relazione ad un fatto di sangue di cui si è ampiamente e a lungo occupata la stampa nazionale e internazionale, ha ritenuto illecita la pubblicazione in più articoli e in un libro di alcune informazioni, riguardanti le abitudini sessuali e lo stato di salute della protagonista della vicenda, ritenute gravemente lesive della sua dignità e della sua riservatezza. Il Tribunale ha condannato la società editrice del quotidiano e la giornalista autrice degli articoli e del libro al risarcimento del danno (sentenza n. 3580 del 20 aprile 2010).

Analoghe considerazioni sono state espresse dal medesimo Tribunale di Milano riguardo alla pubblicazione su di un settimanale di notizie concernenti il domicilio e l'attività lavorativa della ricorrente, coinvolta in un fatto di cronaca quale coniuge del capo di una nota organizzazione criminale. Anche in questo caso all'accertamento della

violazione della normativa sulla protezione dei dati personali è seguita la condanna al risarcimento del danno a favore della parte lesa (sentenza n. 8044 del 21 giugno 2010).

Negli altri casi, l'autorità giudiziaria ha ritenuto non essenziali alla conoscenza dei fatti da parte del pubblico la pubblicazione delle generalità di un minore (Tribunale di Roma, sentenza n. 15605 del 13 luglio 2010), di una persona affetta dalla *cd.* "*influenza suina*" (Tribunale di Roma, sentenza n. 19843 del 5 novembre 2010), della vittima di una rapina (Tribunale di Milano, sentenza n. 13696 del 1 dicembre 2010), di alcune persone fermate per detenzione di sostanze di stupefacenti (Tribunale di Frosinone, sentenza n. 507 del 30 aprile 2010). In tutti i casi è stata pronunciata condanna al risarcimento del danno in favore degli interessati.

Al contrario, il Tribunale di Roma ha ritenuto legittima la messa in onda, all'interno di un programma di informazione calcistica, di un filmato amatoriale che ritraeva un noto calciatore a cui veniva somministrato un farmaco che, benché non vietato dalla normativa *antidoping*, non veniva assunto a scopi terapeutici (sentenza n. 23369 del 24 novembre 2010).

In tal caso, il giudice ha ritenuto che costituisce un tema di indubbia rilevanza sociale quello del miglioramento delle *performance* sportiva realizzata attraverso l'assunzione di farmaci. Nella fattispecie il filmato integra un mero presupposto del necessario soddisfacimento dell'interesse generale alla conoscenza del fenomeno, senza che si possa configurare una lesione della riservatezza del soggetto ripreso, atteso che le immagini divulgate non concernono lo stato di salute dell'interessato, in quanto il farmaco non era stato prescritto a causa di qualche patologia.

Un altro argomento che per la sua attualità e importanza da luogo a numerose controversie è rappresentato dal trattamento dei dati personali effettuato da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti. I giudizi hanno riguardato, in particolare, errate 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).

Tutte le pronunce hanno visto, oltre alla cancellazione dei nominativi degli interessati

dal SIC, anche la condanna al risarcimento del danno dell'istituto o della società che ha effettuato la segnalazione.

I casi decisi hanno riguardato la segnalazione: del fideiussore del terzo debitore in mancanza di prova dell'esistenza di un credito esigibile e del ritardato pagamento da parte del debitore principale (Tribunale di Milano, sentenza n. 13640 del 25 novembre 2010), di un omonimo del soggetto effettivamente inadempiente, con condanna al risarcimento del danno, in solido, anche della società che gestisce il SIC che non aveva verificato l'esattezza dei dati forniti dall'intermediario finanziario (Tribunale di Milano, sentenza n. 5351 del 28 aprile 2010), del sottoscrittore di un contratto di locazione finanziaria, in mancanza di prova dell'effettiva sottoscrizione del contratto (Tribunale di Roma, sentenza n. 6687 del 28 settembre 2010), dell'interessato erroneamente segnalato dall'operatore di una società finanziaria in relazione ad un contratto proposto telefonicamente e non accettato dal ricorrente (Tribunale di Brescia, sentenza n. 3764 del 16 dicembre 2010), di un correntista, in relazione ad un credito residuo a seguito della chiusura del conto corrente, a cui non era stata fornita idonea comunicazione sull'esistenza del debito, che è poi stato immediatamente saldato, mentre l'istituto aveva tardato a procedere alla cancellazione del nominativo dell'interessato dal SIC (Tribunale di Milano, sentenza n. 3716 del 22 marzo 2010).

18.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2010 ha registrato un leggero incremento delle opposizioni a provvedimenti del Garante: a fronte dei 56 ricorsi del 2009, nel 2010 sono state proposte 65 opposizioni. Di queste, 19 si riferiscono a opposizioni ad ordinanze ingiunzioni, con una sostanziale equivalenza rispetto al 2009, nel quale si erano registrate 17 opposizioni di tale natura.

L'Autorità ha avuto notizia di 17 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi.

Quattro pronunce concernono opposizioni ad ordinanze ingiunzioni. Tutte hanno avuto ad oggetto violazioni dell'art. 13 del Codice per omessa o tardiva informativa agli interessati (Tribunale di Arezzo, sentenza n. 197 del 18 febbraio 2010; Tribunale di Milano, sentenza n. 12973 del 16 novembre 2010 e sentenza n. 3972 del 25 marzo 2010;

Tribunale di Varese, sentenza n. 942 del 1° febbraio 2010). Tutte queste pronunce hanno respinto le opposizioni, confermando i provvedimenti del Garante. In un caso la sanzione è stata ridotta a causa della precaria situazione economica della società sanzionata.

Per quanto attiene al trattamento di dati personali effettuato in ambito giornalistico, devono essere segnalate 3 pronunce. In un caso l'Autorità, con *provvedimento* del 25 luglio 2007, aveva respinto il ricorso volto ad ottenere la cancellazione ed il blocco dell'ulteriore trattamento dei dati diffusi in un articolo pubblicato su un quotidiano [doc. *web* n. 1435059]. Il Tribunale di Verona ha respinto l'opposizione proposta dall'interessato in quanto la notizia oggetto dell'articolo è stata ritenuta di indubbia rilevanza pubblica e la sua pubblicazione rientrava nella scelta discrezionale della testata giornalistica (sentenza n. 647 del 9 febbraio 2009).

Un altro caso ha riguardato il *provvedimento* 28 maggio 2009 con il quale il Garante ha respinto il ricorso volto ad ottenere il blocco del trattamento dei dati personali in relazione ad un articolo consultabile, anche in versione informatica, nell'archivio storico di un noto quotidiano [doc. *web* n. 1635910]. Il Tribunale di Milano ha confermato il *provvedimento* del Garante, ritenendo che l'articolo contenga fatti di pubblico interesse e rispetti il limite dell'essenzialità dell'informazione (sentenza n. 4302 del 6 aprile 2010).

Infine, il Tribunale di Milano ha respinto il ricorso avverso il *provvedimento* 3 novembre 2009 con cui una società aveva chiesto l'adozione delle misure necessarie per la cancellazione, rettifica e aggiornamento delle informazioni ricavabili da un motore di ricerca di un noto sito Internet relativamente ad una notizia pubblicata su di un quotidiano *online* inerente una vicenda giudiziaria che aveva coinvolto la ricorrente [doc. *web* n. 1687662]. Il Tribunale di Milano, condividendo le argomentazioni dell'Autorità, ha affermato il difetto di legittimazione passiva della società italiana citata in giudizio, rilevando che la gestione dei servizi del motore di ricerca viene effettuata dalla società capogruppo con sede all'estero, limitandosi la società italiana ad un'attività di supporto nel campo del *marketing* (sentenza n. 10756 del 25 ottobre 2010).

L'esercizio del diritto di accesso ai dati personali ha riguardato 5 pronunce.

In 2 casi si è trattato di un'istanza di accesso ai dati relativi a una persona defunta.

Nel primo caso, l'erede aveva chiesto di poter avere accesso al nominativo del beneficiario di una polizza assicurativa sottoscritta dal *de cuius*. Il Tribunale di Roma, conformemente a quanto stabilito dal Garante con *provvedimento* 26 marzo 2009 [doc. *web* n. 1608042], ha ritenuto che l'impresa assicuratrice, in qualità di titolare del trattamento, ha l'obbligo di fornire all'erede tutte le informazioni relative alle polizze stipulate dal dante causa, ma con esclusivo riferimento agli atti contenenti i dati personali del medesimo e non anche di terzi beneficiari che non vi abbiano acconsentito (sentenza n. 13713 del 15 dicembre 2010).

Nel secondo caso il Garante, con *provvedimento* 28 settembre 2006, ha ritenuto applicabile la disciplina dell'accesso ai dati personali dettata dal Codice alla richiesta rivolta dall'erede all'istituto bancario di avere copia degli assegni rilasciati dal *de cuius*, [doc. *web* n. 1348677]. Il Tribunale di Pisa, sezione distaccata di Pontedera, ha, invece, stabilito che la movimentazione bancaria relativa ai suddetti titoli di credito non contiene dati personali e ha ritenuto applicabile la disciplina disposta dal t.u. bancario in materia di accesso alla documentazione bancaria (sentenza n. 173 del 14 aprile 2010).

Altre 2 pronunce hanno riguardato l'accesso ai dati personali in tema di lavoro.

Nel primo caso (sentenza n. 462 del 24 febbraio 2010), il Tribunale di Lecce ha respinto il ricorso proposto avverso il *provvedimento* 19 dicembre 2008 [doc. *web* n. 1582051], con il quale l'Autorità ha ordinato alla società datrice di lavoro di consentire al dipendente l'accesso ai dati personali che lo riguardano inerenti il rapporto di lavoro.

Nel secondo caso, il Garante, con *provvedimento* 21 gennaio 2010, ha ordinato ad una società di consentire ad una dipendente licenziata l'accesso alla propria casella di posta elettronica presso la sede lavorativa, nonché di trasporre i dati personali ivi contenuti su supporto cartaceo o informatico in presenza di personale appositamente incaricato dalla resistente [doc. *web* n. 1701577]. Il Tribunale di Milano ha confermato il *provvedimento* del Garante, ritenendo che le informazioni contenute nelle e-mail inviate e ricevute sulla casella di posta elettronica aziendale dal dipendente costituiscono dati personali del medesimo, che in relazione ad essi è quindi possibile chiedere l'accesso ai sensi dell'art. 7 del Codice e che le modalità di accesso delineate nel *provvedimento* sono idonee a preservare la riservatezza dell'azienda (sentenza n. 8188 del 2 settembre 2010).

Con altra pronuncia, il Tribunale di Milano ha confermato il *provvedimento* 25 marzo 2008 con il quale il Garante [doc. *web* n. 1507012] ha respinto, in quanto presentata oltre il termine previsto dalla legge, la richiesta di una società volta ad ottenere da un gestore di telefonia mobile, al fine della difesa in giudizio, i dati relativi al traffico telefonico di un'utenza (sentenza n. 13750 del 30 novembre 2010).

Una decisione ha riguardato la richiesta di un privato nei confronti di un istituto bancario, di prescrivere tutte le misure necessarie per il ripristino dei diritti del ricorrente, di conoscere dell'esistenza, della conservazione e delle modalità di gestione dei propri dati personali presso il suddetto istituto e di dichiarare l'illegittimità della diffusione dei dati e la cessazione del comportamento illegittimo. Il Tribunale di Bologna, nel respingere il ricorso, ha confermato il provvedimento 18 aprile 2008, rilevando la genericità e l'indeterminatezza della domanda, nonché l'assenza di violazioni della normativa in materia di protezione dei dati personali (sentenza n. 7997 del 4 novembre 2010).

In tema di misure di sicurezza, il Garante, con *provvedimento* 26 marzo/2 aprile 2009 ha prescritto ad un'associazione, in relazione ad un illecito utilizzo dei dati degli iscritti a fini propagandistici-elettorali da parte di un terzo, di adottare misure idonee a contenere i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, e di designare gli incaricati del trattamento [doc. *web* n. 1606059]. Il Tribunale di Roma ha confermato integralmente il provvedimento con sentenza n. 19186 del 7 ottobre 2010.

Un'ulteriore pronuncia del Tribunale di Roma (sentenza n. 24978 del 6 aprile 2010) ha accolto il ricorso proposto da una società che gestisce banche dati nell'ambito della *cd.* "*business information*", ritenendo che alcune specifiche informazioni riferite ad un soggetto censito nella banca dati costituiscono dati pertinenti al medesimo e non eccedenti lo scopo del trattamento, e annullando il *provvedimento* 19 dicembre 2008 [doc. *web* n. 1583124].

Con un'altra decisione il Tribunale di Grosseto, annullando il *provvedimento* 14 ottobre 2009 [doc. *web* n. 1658058], ha accolto il ricorso presentato da un dirigente scolastico, ritenendo lecito il trattamento dei dati personali di un'insegnante, contenuti in un verbale

di accertamento sanitario redatto dalla commissione medica di verifica, consistito nella trasmissione, in busta chiusa, dei dati all'istituzione scolastica individuata come competente (sentenza n. 502 del 11 novembre 2010).

Infine, come già riportato (*supra*, par. 18.2.), il Tribunale di Perugia, sezione distaccata di Todi, ha dichiarato la propria incompetenza territoriale in favore del Tribunale di Roma, in applicazione dell'art. 152, comma 2, del Codice, che prevede la competenza a conoscere della controversia del Tribunale del luogo ove ha la sede legale il titolare del trattamento (sentenza n. 15 del 19 febbraio 2008).

18.5. L'INTERVENTO DEL GARANTE NEI GIUDIZI RELATIVI ALL'APPLICAZIONE DEL CODICE

Conformemente agli indirizzi giurisprudenziali e al parere 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, nel quale l'Autorità ha 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 in merito agli esiti, il Garante è intervenuto in un caso in cui aveva ricevuto da un Internet *service provider* la segnalazione di una presunta attività di monitoraggio del traffico telematico dei suoi utenti da parte della Federazione antipirateria audiovisiva, desunta dagli elementi prodotti dalla Federazione nel giudizio di urgenza promosso nei confronti della segnalante presso il Tribunale civile di Roma per la asserita illecita acquisizione da parte degli utenti di opere audiovisive protette tramite la rete Internet.

L'intervento del Garante ha riguardato i profili della vicenda attinenti alla protezione dei dati personali, e in particolare:

- la possibilità che gli elementi posti a fondamento del ricorso giudiziale della Federazione fossero il risultato di un illecito trattamento di dati personali degli utenti del *provider* e, come tali, inutilizzabili, anche in sede giudiziaria (art. 11, comma 2, del Codice);
- la possibilità che la richiesta della ricorrente al giudice adito di ordinare al *provider* di comunicare alle autorità di pubblica sicurezza tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette si sostanziasse nell'obbligo per il *provider* di effettuare un monitoraggio delle attività compiute in rete dai propri utenti e quindi di compiere un trattamento di dati personali illecito, per la sua contrarietà alle vigenti disposizioni, nazionali e comunitarie, in tema di tutela della riservatezza; trattamento che il Garante aveva già espressamente vietato (*Provv.* 10 gennaio 2008 [doc. *web* n. 1524263]).

Con ordinanza depositata il 15 aprile 2010 il Tribunale di Roma ha accolto parzialmente il ricorso cautelare della Federazione, ma ha confermato, nella sostanza, la tesi principale sostenuta dall'Autorità secondo la quale non è ammissibile, allo stato della legislazione in materia di protezione dei dati personali, che il giudice civile ordini ad un *provider* di monitorare la navigazione in rete dei propri utenti, acquisendo dati anche sui siti visitati, al fine di individuare eventuali comportamenti violativi del diritto di autore.

19. L'ATTIVITÀ ISPETTIVA E LE SANZIONI

19.1. LA PROGRAMMAZIONE DELL'ATTIVITÀ ISPETTIVA

Nel 2010 sono state effettuate 474 ispezioni sulla base dei programmi ispettivi semestrali disposti dall'Autorità.

Come evidenziato anche nelle precedenti Relazioni, l'attività di controllo è stata essenzialmente volta a verificare il rispetto dei principali adempimenti previsti dal Codice da parte di:

- enti pubblici o aziende che gestiscono banche dati di particolare rilevanza o dimensioni, in cui vengono trattati dati di ampie categorie di interessati (ad es., anagrafe tributaria, patronati, enti previdenziali, banche, comuni con riferimento all'anagrafe della popolazione, società che gestiscono banche dati per finalità di *marketing*);
- soggetti che effettuano trattamenti di dati sensibili e, in particolare, idonei a rivelare lo stato di salute degli interessati (ad es., ospedali e cliniche private e trattamenti relativi alla realizzazione del fascicolo sanitario elettronico);
- società che effettuano trattamenti di dati personali facendo ricorso a particolari tecnologie (ad es., trattamento di dati biometrici);
- società che effettuano trattamenti di dati per i quali il Codice prevede l'obbligo di notificazione (ad es., attività di profilazione o di gestione di banche dati relative al rischio di solvibilità economica, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti).

Le linee di indirizzo dell'attività ispettiva sono stabilite, con cadenza semestrale, dal Collegio attraverso delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire.

Sulla base di tali criteri, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche attraverso la rivista settimanale (*Newsletter*) pubblicata sul sito *www.garanteprivacy.it*.

Lo svolgimento dell'attività ispettiva permette di acquisire importanti elementi di valutazione in ordine ad alcuni importanti profili quali il grado di adeguamento alla legge di

categorie omogenee di operatori, la sussistenza di fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali nonché la verifica dell'impatto dei provvedimenti adottati.

In tal modo l'attività ispettiva acquisisce una valenza conoscitiva e di indirizzo oltre che repressiva. Nell'anno 2010, il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva fosse indirizzata a:

- trattamenti di dati personali effettuati presso istituti di credito relativamente alla legittimità della consultazione e del successivo utilizzo di dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- trattamenti di dati personali effettuati da società che gestiscono pagamenti attraverso carte di credito;
- trattamenti di dati personali effettuati da enti previdenziali mediante i propri sistemi informativi;
- trattamenti di dati personali effettuati dall'amministrazione finanziaria mediante il sistema informativo della fiscalità (anagrafe tributaria);
- trattamenti di dati personali effettuati da enti pubblici in relazione all'adozione dei regolamenti sui dati sensibili e alla realizzazione del fascicolo sanitario elettronico;
- trattamenti di dati personali in relazione alla formazione e commercializzazione di banche dati, per finalità di *marketing* effettuato anche attraverso l'invio di *Sms* ed *Mms*.

Con riferimento, invece, al secondo semestre (luglio-dicembre), l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- trattamenti di dati personali effettuati da società che gestiscono pagamenti attraverso carte di credito;
- trattamenti di dati personali effettuati da enti previdenziali mediante i propri sistemi informativi;
- trattamenti di dati personali effettuati da società attraverso sistemi di rilevamento biometrici;

- trattamenti di dati personali in relazione alla formazione e commercializzazione di banche dati per finalità di *marketing* effettuato anche attraverso l'invio di *Sms* ed *Mms*;
- trattamenti di dati personali effettuati dai comuni con riferimento all'anagrafe della popolazione residente.

Nel periodo di riferimento sono state altresì effettuate:

- verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- altre verifiche di iniziativa concernenti, in particolare, l'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- verifiche 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, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

In base ai regolamenti dell'Autorità, l'istruttoria preliminare relativa alle ispezioni effettuate d'ufficio sulla base dei criteri fissati dal Collegio spetta al dipartimento attività ispettive e sanzioni.

Effettuati gli accertamenti sulle presunte violazioni, il dipartimento procede direttamente alle contestazioni di sanzioni amministrative e inoltra gli atti alla competente unità organizzativa per il seguito di trattazione, che concerne profili diversi dall'applicazione di sanzioni (adozione di provvedimenti prescrittivi o inibitori).

Il dipartimento attività ispettive e sanzioni cura, altresì, i controlli nell'ambito delle istruttorie preliminari e dei procedimenti amministrativi comunque avviati presso altre unità organizzative (di norma sulla base di segnalazioni, ricorsi o reclami), cui è restituito l'esito per la successiva trattazione.

19.2. 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 nel dettaglio riferito nelle precedenti edizioni (cfr., da ultimo, *Relazione* 2009, p. 240 ss.), evidenziando la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente a effettuare gli accertamenti, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Come già accade da alcuni anni, le informazioni e i documenti acquisiti nell'ambito degli accertamenti sono stati trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Laddove siano emerse violazioni penali o amministrative, la Guardia di finanza ha direttamente segnalato la notizia di reato all'autorità giudiziaria e contestato la sanzione amministrativa.

Si è registrato inoltre un importante coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, gruppi, compagnie e tenenze) e un rafforzamento del ruolo di coordinamento del Nucleo speciale *privacy* rispetto all'attività subdelegata a tali reparti.

In tal modo l'Autorità ha fruito di un dispositivo di controllo flessibile ed articolato, idoneo a espletare l'attività di controllo sul territorio in modo più efficace e tempestivo.

19.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2010 sono state effettuate, suddivise per settore, le seguenti attività ispettive:

- 85 controlli nei confronti di cliniche private, ospedali e case di cura pubbliche, centri di chirurgia estetica e società che gestiscono cartelle cliniche che trattano dati relativi alla salute, con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza;
- 35 controlli nei confronti di centri di riabilitazione, con riferimento al trattamento dei dati degli utenti;
- 34 controlli nei confronti di società telefoniche, *dealer* e altri soggetti, con riferimento

alle modalità di attivazione delle schede telefoniche (*Sim card*), al fine di verificare il rispetto delle prescrizioni contenute nel *provvedimento* 16 febbraio 2006 [doc. *web* n. 1242592] in tema di servizi telefonici non richiesti;

- 30 controlli nei confronti di esercizi ricreativi, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 25 controlli nei confronti di soggetti vari che hanno effettuato la notificazione al registro generale dei trattamenti;
- 20 controlli nei confronti di scuole ed istituti di formazione, con riferimento al trattamento dei dati dei discenti effettuato anche mediante raccolte di dati via *web*;
- 20 controlli nei confronti di soggetti fornitori di servizi di ricezione ed ospitalità, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 17 società di noleggio, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 14 controlli nei confronti di società che commercializzano banche dati a terzi per finalità di *marketing* anche attraverso l'invio di *Sms*, *Mms* ed e-mail, volti a rilevare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati;
- 13 controlli nei confronti di chiromanti, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 11 controlli nei confronti di università *online*, con riferimento al trattamento dei dati degli studenti;
- 10 controlli nei confronti di istituti di credito, con riferimento alla legittimità della consultazione e del successivo utilizzo dei dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- 8 controlli nei confronti di società che effettuano attività di *marketing* attraverso l'invio di fax, volti a rilevare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati per tali finalità;

- 3 controlli nei confronti di enti previdenziali e patronati che utilizzano i sistemi informativi dei predetti enti volti a rilevare la liceità dei trattamenti e le misure di sicurezza adottate;
- 3 controlli nei confronti di società che gestiscono pagamenti attraverso carte di credito con riferimento alle modalità di trattamento dei dati dei clienti;
- 2 controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante l'anagrafe tributaria volti a rilevare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di comuni con riferimento ai trattamenti di dati personali effettuati attraverso l'anagrafe della popolazione residente e l'anagrafe degli italiani residenti all'estero.

A questi si aggiungono i 109 controlli effettuati nei confronti di altri soggetti, per esigenze istruttorie connesse a specifiche segnalazioni pervenute all'Autorità.

In relazione a quanto emerso dagli accertamenti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

Tra i più rilevanti, in ordine cronologico, si segnalano:

- il *provvedimento* con il quale il Garante, a conclusione dell'istruttoria svolta nei confronti di INPS, INPDAP, ENPALS, AVCP, camere di commercio ed AGEA, ha prescritto all'Agenzia delle entrate specifiche misure, di carattere prevalentemente tecnico, idonee ad assicurare che l'accesso all'anagrafe tributaria effettuato dai predetti enti attraverso la nuova classe di *web* service predisposta dall'Agenzia avvenga nel rispetto del Codice. Nel medesimo *provvedimento* è stata altresì prescritta ai predetti enti, utilizzatori dei *web* service dell'Agenzia delle entrate, l'adozione di ulteriori misure da seguire nella fase di integrazione di tali strumenti nell'ambito dei propri applicativi (*Provv.* 26 marzo 2010 [doc. *web* n. 1713453]);
- il nuovo *provvedimento* generale in materia di videosorveglianza, di cui si è riferito nella *Relazione* 2009, p. 25 ss. (*Provv.* 8 aprile 2010 [doc. *web* n. 1712680]);

- il *provvedimento* con il quale il Garante ha vietato ad una società che gestisce un portale che promuove la prenotazione di servizi turistici qualunque trattamento a fini di profilazione effettuato senza il consenso preventivo, specifico e informato degli interessati ed ha prescritto alla medesima società di rendere conforme alle disposizioni del Codice l'informativa data attraverso il proprio sito *web* (*Provv.* 8 aprile 2010 [doc. *web* n. 1721205]);
- il *provvedimento* con il quale il Garante ha disposto il blocco del trattamento dei dati personali effettuato da una ditta individuale a mezzo videosorveglianza presso un proprio punto vendita, in attesa dell'eventuale espletamento delle procedure previste dalla l. n. 300/1970 (Statuto dei lavoratori) per i casi in cui tali strumenti siano idonei a configurare un controllo a distanza dei lavoratori (*Provv.* 10 giugno 2010 [doc. *web* n. 1736167]);
- il *provvedimento* con il quale il Garante ha disposto il blocco del trattamento delle immagini riprese nelle aree interne, per mezzo di un sistema di videosorveglianza, da un centro per la riabilitazione, nelle more dell'espletamento delle procedure previste dalla l. n. 300/1970 (Statuto dei lavoratori) per i casi in cui tali strumenti siano idonei a configurare un controllo a distanza dei lavoratori, invitando il medesimo soggetto ad adottare, medio tempore, adeguate misure alternative per garantire l'incolumità di pazienti, operatori sanitari e dipendenti (*Provv.* 24 giugno 2010 [doc. *web* n. 1738396]);
- il *provvedimento* con il quale il Garante ha vietato a un importante gruppo societario, operante nel settore radiofonico e nella gestione dei siti Internet delle proprie emittenti e dei concorsi a premi da queste effettuati, il trattamento di dati personali degli utenti raccolti attraverso i siti *web* delle emittenti, finalizzato all'invio di comunicazioni commerciali, ad operazioni di profilazione e alla comunicazione a terzi dei dati personali senza il necessario consenso specifico, libero e informato. Nel medesimo *provvedimento* sono state altresì prescritte le misure necessarie per rendere conforme il trattamento alle disposizioni del Codice con riferimento alle modalità con le quali viene resa l'informativa, al relativo contenuto e agli adempimenti in tema di notificazione per i trattamenti effettuati a fini di profilazione (*Provv.* 22 luglio 2010 [doc. *web* n. 1741988]);

- il *provvedimento* con il quale l'Autorità ha tra l'altro prescritto ad una società, operante nel settore del mailing postale per finalità di comunicazione commerciale e di *marketing*, di pubblicare almeno una volta l'anno l'informativa prevista dall'art. 13 del Codice, con la specifica ed aggiornata indicazione delle fonti da cui i dati sono tratti, compresa l'ipotesi in cui gli stessi siano acquisiti da società terze, tramite un avviso su tre quotidiani ad ampia diffusione nazionale, nonché di pubblicare la medesima informativa anche sul proprio sito *web*, in un'apposita sezione dedicata alla *privacy*, adeguatamente evidenziata in autonomi riquadri e di immediata consultazione (*Provv.* 16 dicembre 2010 [doc. *web* n. 1781973]).

19.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

19.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

A seguito delle ispezioni effettuate e, più in generale, dall'esame degli atti delle istruttorie effettuate dall'Autorità si sono rilevati gli estremi per l'invio all'autorità giudiziaria di 55 informative (di cui 25 direttamente da parte dell'Autorità e 30 da parte della Guardia di finanza).

Le segnalazioni relative a presunte violazioni penali hanno riguardato:

- in 34 casi la mancata adozione delle misure minime di sicurezza;
- in 7 casi l'inosservanza di un *provvedimento* del Garante;
- in 4 casi la falsità nelle dichiarazioni e notificazioni al Garante;
- in 3 casi il trattamento illecito dei dati;
- in 7 casi violazioni della l. n. 300/1970 (Statuto dei lavoratori) ora punite come reato dall'art. 171 del Codice, o violazioni penali previste da disposizioni non contenute nel Codice in materia di protezione dei dati personali.

Come dimostrano i dati sopra riportati, la violazione penale più frequentemente accertata riguarda il mancato rispetto delle disposizioni concernenti le misure minime di sicurezza che devono essere adottate da coloro che trattano dati personali (titolari, responsabili ed incaricati) per assicurare agli interessati di cui trattano i dati un livello di sicurezza adeguato predefinito dalle norme.

Come noto, in base all'art. 169, comma 2, del Codice, nel caso in cui venga rilevata

una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza (Allegato B. al 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 alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazione in ordine all'estinzione del reato.

Con riferimento a questa complessa procedura, i procedimenti definiti nell'anno 2010 connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, sono stati 17 e hanno determinato il pagamento all'Autorità di 457.500 euro da parte delle persone responsabili delle violazioni.

19.4.2. Sanzioni amministrative

A seguito delle ispezioni effettuate e delle istruttorie curate dall'Ufficio, sono stati avviati 424 procedimenti sanzionatori amministrativi (di cui 220 direttamente dal Garante e 204 da parte della Guardia di finanza e di altri organi accertatori).

Le sanzioni amministrative contestate hanno riguardato le seguenti violazioni:

- omessa o inidonea informativa (239);
- trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (124);
- omessa informazione o esibizione al Garante (19);
- omessa o incompleta notificazione (20);
- inosservanza di un *provvedimento* del Garante (12);
- sanzioni in materia di conservazione dei dati di traffico (4);
- più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (6).

Sotto il profilo economico, le sanzioni contestate nell'anno 2010 prevedono la possibilità di applicare pene pecuniarie da un minimo di circa 5.200.000 euro a un massimo di circa 31.100.000 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.

Complessivamente le entrate relative all'attività sanzionatoria per l'anno 2010 sono effettivamente state pari a 3.809.000 euro in relazione a:

- 319 procedimenti sanzionatori spontaneamente definiti mediante pagamento dai contravventori (per un importo di 3.046.001 euro);
- 132 ordinanze-ingiunzione adottate dall'Autorità sulla base dell'esame delle memorie e delle audizioni delle parti (per un importo di 306.400 euro);
- 17 ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (per un importo di 457.500 euro).

Occorre evidenziare che la gran parte dei procedimenti sanzionatori definitisi nell'anno 2010 riflette ancora violazioni commesse in epoca anteriore all'entrata in vigore del d.l. 30 dicembre 2008, n. 207 (convertito nella l. 27 febbraio 2009, n. 41), e per le quali l'ammontare delle pene pecuniarie era sensibilmente inferiore a quello attuale.

Sono stati 86 i procedimenti sanzionatori definitisi in senso favorevole al contravventore con l'adozione di ordinanze di archiviazione.

Come evidenziano i dati, il maggior numero di sanzioni erogate ha riguardato la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali.

In particolare, tale violazione è stata riscontrata sui siti *web*, a fronte di una raccolta dei dati effettuata mediante *form* e spesso finalizzata a raccogliere richieste di utenti. Tale circostanza ha indotto i gestori dei siti Internet a ritenere che non fosse necessario indicare l'informativa in calce ai predetti *form*, sul presupposto che i dati erano forniti

dagli interessati volontariamente. L'omessa/inidonea informativa, in alcune ipotesi di comunicazione di dati personali a terzi, è stata contestata sia alla società che, avendo raccolto i dati dell'interessato, li ha poi trasmessi a un *partner* commerciale senza informare l'interessato, sia al *partner* commerciale che, avendoli ricevuti, li ha trattati (ad es., per l'invio di comunicazioni commerciali) senza rendere l'informativa agli interessati nei termini previsti dalle disposizioni. Frequenti anche le contestazioni relative alla mancata predisposizione delle informative in casi di trattamento di dati mediante sistemi di videosorveglianza.

Numerose sono state altresì le sanzioni per illecito trattamento amministrativo di dati personali di cui all'art. 162, comma 2-*bis*, del Codice, soprattutto per violazione dell'obbligo del consenso al trattamento da parte dell'interessato e per omissioni nell'adozione delle misure minime di sicurezza. Per il primo aspetto, le violazioni hanno interessato soprattutto le società che effettuano attività di *marketing* mediante fax, e-mail, *Sms*. Anche a fronte di un'informativa completa, i soggetti sanzionati non avevano documentato il consenso libero e informato degli interessati per tale specifica finalità. Per le misure di sicurezza, la violazione più frequentemente accertata è da ricondurre alla mancata designazione degli incaricati del trattamento, che comporta la non applicazione di tutte le misure di sicurezza che il disciplinare tecnico di cui all'Allegato B. del Codice riconduce all'attività degli incaricati medesimi e, segnatamente, delle regole 1-10 (autenticazione informatica), 12-15 (adozione di un sistema di autorizzazione), 22 e 23 (dati sensibili contenuti in supporti rimovibili), 27 (dati comuni contenuti in supporti cartacei), 28 e 29 (dati sensibili contenuti in supporti cartacei). Al riguardo è opportuno evidenziare che la mancata designazione degli incaricati del trattamento non costituisce un mero inadempimento formale, in quanto la parte più significativa delle misure di sicurezza da adottarsi per il trattamento dei dati personali è strettamente correlata all'attività degli incaricati stessi, (ovvero di coloro che ordinariamente operano sui dati personali) e mira a fornire loro le istruzioni per il corretto trattamento dei dati, rendendoli al contempo consapevoli delle connesse responsabilità anche attraverso il loro inserimento in specifici processi formativi in materia di *privacy* (prescritti dalla regola 19.6 del citato disciplinare tecnico in relazione all'adozione del documento programmatico sulla sicurezza).

Numerose sono state anche le contestazioni nei confronti di coloro che non hanno fornito risposta alle richieste istruttorie fatte dall'Autorità. In questi casi, di massima, oltre alla contestazione della sanzione si è proceduto anche a disporre un accertamento *in loco*, in linea di massima delegato al Nucleo speciale *privacy* della Guardia di finanza, al fine di acquisire i necessari elementi istruttori.

Assai significativi per l'importo della pena pecuniaria (da 60.000 a 180.000 euro), ancorché non particolarmente numerosi, sono invece stati i casi di inosservanza dei provvedimenti del Garante.

In un caso si è trattato di una società che ha contravvenuto al divieto del Garante di inviare comunicazioni commerciali e promozionali senza che risultasse comprovato un consenso libero ed informato degli interessati; in altri casi, invece, non sono stati osservati i provvedimenti relativamente a trattamenti di dati personali tratti da elenchi telefonici. Rilevante infine anche il caso relativo alla violazione, da parte di un'emittente televisiva, di un divieto adottato dal Garante in relazione alla messa in onda di dati personali relativi a casi di adozioni affrontati nel corso delle puntate di una trasmissione televisiva.

Nell'ambito delle attività ispettive effettuate per verificare il rispetto dei termini di conservazione dei dati di traffico telefonico e telematico da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, sono state rilevate 4 violazioni di quanto previsto dall'art. 132 del Codice, che impone specifici limiti temporali di conservazione di tali dati per finalità di prevenzione e accertamento dei reati.

In un caso il fornitore del servizio conservava dati di traffico dei propri clienti risalenti all'anno 2001, senza aver mai provveduto a cancellarli o introdotto limiti di conservazione.

In un altro caso, la violazione è stata accertata in relazione alla conservazione di dati (l'oggetto dei messaggi di posta elettronica) che non rientravano, sulla base di quanto previsto dall'art. 3 del d.lgs. n. 109/2008, tra quelli da conservare per le finalità di cui all'art. 132 del Codice e che, essendo potenzialmente correlati al contenuto della comunicazione, non potevano essere conservati.

In un terzo caso, è emerso che veniva conservato tra i dati di traffico anche l'indirizzo *IP* di destinazione in relazione alla navigazione Internet effettuata dagli abbonati al servizio,

benché l'art. 3 del d.lgs. n. 109/2008 non includa, tra le categorie di dati da conservare per le finalità di cui all'art. 132 del Codice, tale informazione (anch'essa considerata potenzialmente correlata al contenuto della comunicazione).

Da segnalare infine i primi casi di procedimenti sanzionatori avviati con riferimento alla disposizione contenuta nell'art. 164-*bis*, comma 2, del Codice per le violazioni commesse da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni. Si è trattato di società che hanno commesso reiterate violazioni sanzionate dal Codice, in relazione ad un numero assai rilevante di dati personali organizzati all'interno di banche dati, cedute a terzi per essere utilizzate per finalità di *marketing*. Tali banche dati costituivano un archivio aggiornato di informazioni relative a una quota rappresentativa della popolazione e degli operatori economici presenti nel territorio italiano e, quindi, sono state considerate, sulla base di quanto previsto dall'art. 164-*bis*, comma 2, del Codice "*banche dati di particolare rilevanza o dimensioni*".

Sul nuovo apparato sanzionatorio e sulle disposizioni procedurali si fa rinvio alla *Relazione* 2009, p. 249 ss.

20. Le relazioni internazionali

Sono stati celebrati nel periodo di riferimento il trentennale delle linee-guida dell'OCSE sulla protezione e i flussi transfrontalieri dei dati (adottate il 23 settembre 1980), nonché il trentennale della Convenzione 108 del Consiglio d'Europa (adottata il 28 gennaio 1981).

Tale ricorrenza ha costituito una preziosa occasione di riflessione, per verificare se gli strumenti e le strategie operativi dall'inizio degli anni '80, ma concepiti negli anni '70, possano considerarsi ancora attuali, anche alla luce del profondo mutamento istituzionale e normativo nell'Unione europea conseguente all'entrata in vigore del Trattato di Lisbona e ai lavori in corso per la revisione della Direttiva n. 95/46/CE.

Come già indicato nella precedente *Relazione* annuale (p. 253), con il Trattato di Lisbona la protezione dei dati personali ha acquisito un nuovo e diverso ruolo: da un lato, le disposizioni della Carta dei diritti fondamentali –che, com'è noto, hanno introdotto il diritto fondamentale delle persone alla tutela dei propri dati personali (art. 8), affiancandolo al diritto alla riservatezza (art. 7)– sono divenute giuridicamente vincolanti; dall'altro, è emersa l'esigenza di pervenire ad un quadro uniforme di princìpi, come previsto dall'art. 16 del Trattato sul funzionamento dell'Unione europea, pur con i contemperamenti previsti dalle dichiarazioni allegate al Trattato.

La Commissione europea ha adottato, il 4 novembre 2010, la Comunicazione intitolata "*Un approccio globale alla protezione dei dati personali in Europa*" in cui traccia le linee di fondo secondo le quali intende articolare il proprio intervento, anche con il conforto dell'esperienza delle autorità di protezione dei dati riunite nel Gruppo Art. 29, nell'intento di presentare, entro il primo semestre del 2011, la proposta di revisione della Direttiva n. 95/46/CE.

Le innovazioni tecnologiche e il mutato scenario economico-sociale (impatto delle nuove tecnologie quali il *cloud computing*; l'accentuata globalizzazione nel trasferimento dei dati; l'utilizzo di tecniche di *behavioural advertising* sempre più sofisticate) oltre che le già menzionate innovazioni del quadro giuridico determinano, ad avviso della

Commissione, l'esigenza di mettere a punto una cornice normativa coerente e comune per il trattamento di dati personali nel contesto di tutte le politiche dell'Unione europea.

Fondamentali saranno, pertanto, gli interventi sulle definizioni contenute nella direttiva, quali la definizione di "*dato personale*" (che potrebbe includere i dati sulla geo-localizzazione ed altri non ancora contemplati dalla direttiva), nonché di "*dato sensibile*" e di "*consenso informato*". Ciò al fine di assicurare la certezza del diritto per i titolari del trattamento e gli interessati; di aumentare il grado di trasparenza che i titolari del trattamento devono garantire agli interessati –eventualmente anche estendendo l'obbligo (previsto dalla Direttiva e-*privacy* n. 2002/58/CE di recente modificata) di segnalazione delle violazioni degli obblighi in materia di protezione dati da cui possano derivare danni agli interessati ("*general personal data breach notification*")– di permettere un controllo più effettivo, da parte degli stessi interessati sul trattamento dei propri dati (diritto di accesso, rettifica, blocco, cancellazione) e di assicurare che vengano comminate sanzioni adeguate in caso di violazione della normativa posta a presidio della *privacy*.

Da un punto di vista più generale, la proposta della Commissione si prefigge alcuni importanti obiettivi quali: la riforma del quadro regolamentare che garantisca maggiore armonizzazione tra le normative nazionali di recepimento; la revisione e semplificazione del sistema di notifica; la certezza giuridica in merito al diritto nazionale applicabile; l'osservanza delle norme da parte dei titolari del trattamento, anche attraverso sistemi di controllo e responsabilità interni (*cd.* "*accountability*").

Quanto al trattamento dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale, la Comunicazione ha sottolineato che la Decisione-quadro 2008/977/GAI del Consiglio presenta non poche criticità (applicazione limitata ai dati trasmessi nell'ambito della cooperazione tra Stati membri, e non estesa a trattamenti meramente interni ad uno stesso Stato membro; armonizzazione di tipo "minimo"; problemi di coerenza con altri strumenti legislativi). La riforma del quadro regolamentare si propone di superare tali criticità estendendo, per quanto possibile e tenuto conto delle specificità del settore, le regole generali previste dalla novellata direttiva.

In materia di trasferimento dei dati extra-UE –uno dei temi più critici– la proposta ha

come obiettivo il riesame delle procedure per la valutazione del livello di "adeguatezza" degli Stati terzi ("*adequacy procedure*"), l'introduzione e disciplina delle clausole contrattuali *standard* e delle "norme vincolanti d'impresa" (BCR) per i trasferimenti infragruppo, il rafforzamento della cooperazione con organismi internazionali attivi sullo stesso tema (OCSE, Consiglio d'Europa, Nazioni Unite).

La Commissione ha altresì indicato la necessità, per una applicazione effettiva delle norme di protezione dei dati, di un rafforzamento dell'assetto istituzionale, ribadendo l'essenzialità del ruolo delle autorità nazionali di protezione dei dati personali istituite dall'art. 28 della Direttiva n. 95/46/CE, cui deve essere garantita, come di recente indicato dalla Corte di giustizia UE (sentenza 9 marzo 2010, in C-518/07, Commissione contro Repubblica federale di Germania) piena indipendenza ed attribuiti competenze, poteri e mezzi adeguati alle funzioni da svolgere. In merito al coordinamento delle autorità nazionali di protezione dati, oggi svolto dal Gruppo Art. 29, la Commissione ha menzionato la possibile istituzione di una procedura per assicurare la coerenza del coordinamento medesimo nel mercato interno sotto l'autorità della stessa Commissione.

Il lavoro del Gruppo Art. 29, come più diffusamente indicato *infra* (par. 20.2.) ha registrato un'ulteriore crescita, grazie all'ampliamento delle competenze anche ai trattamenti dei dati nell'area dell'ex *cd.* "terzo pilastro".

Occorre inoltre evidenziare il maggiore ruolo riconosciuto al Parlamento europeo, anche in ragione dei nuovi poteri attribuitigli dal Trattato di Lisbona, e la concreta possibilità di scambi diretti di informazioni e opinioni tra le autorità di protezione dei dati personali riunite nel Gruppo Art. 29.

I contributi forniti dal Parlamento hanno riguardato in particolare accordi internazionali in settori particolarmente delicati, quali l'accordo Unione europea-Stati Uniti per l'uso dei dati *Swift*, nonché il rinnovo degli accordi con Stati Uniti, Australia e Canada concernenti l'uso dei dati personali dei passeggeri aerei ("*Passenger name records*" - *PNR*).

L'entrata in vigore del Trattato di Lisbona ha comportato, altresì, il progressivo e sempre maggiore coinvolgimento dei parlamenti nazionali nella *cd.* "*fase ascendente*" del procedimento legislativo comunitario. I parlamenti nazionali, infatti, avvalendosi, in particolare,

dei poteri ad essi conferiti dall'art. 12 del Trattato sull'Unione europea e dal Protocollo sul ruolo dei parlamenti nazionali nell'Unione europea, potranno valutare con maggiore incisività il rispetto dei princìpi di sussidiarietà e di proporzionalità di ogni proposta legislativa, ivi incluse quelle che abbiano un impatto sul diritto alla protezione dei dati personali.

20.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Conferenza internazionale delle autorità di protezione dati Gerusalemme 2010

La Conferenza internazionale si è tenuta a Gerusalemme dal 27 al 29 ottobre 2010; la parola chiave è stata "*Generazioni*", riferita sia alle "nuove generazioni" di utenti della Rete, sia alle tecnologie e regole di "nuova generazione", specie in relazione allo sviluppo della "*privacy by design*". Le autorità di protezione dati e alcuni rappresentanti della comunità scientifica si sono confrontati sui cambiamenti provenienti dal *cyberspazio*. Particolare attenzione è stata rivolta alla percezione della *privacy* da parte degli utenti della Rete più giovani. Una serie di sessioni a tema, organizzate parallelamente a quella plenaria, hanno riguardato i temi dell'*accountability*, della protezione dei dati *online*, del *cd.* "Internet delle cose" ("*Internet of things*"), del rapporto tra la *privacy* e la tutela dei diritti di autore e dei consumatori, del *cd.* "*diritto all'oblio*" ("*right to be forgotten*"), nonché dell'accesso dei governi ai dati in possesso di soggetti privati.

Al Garante italiano è stato affidato il compito di presiedere la sessione dedicata al consenso come presupposto legittimante l'uso dei dati personali. Punto di partenza del dibattito è stata la necessità di ripensare il consenso –sia nel mondo *offline*, sia in Internet– affinché esso continui ad avere un ruolo realmente efficace nel sistema di protezione dei dati. Il Presidente dell'Autorità ha sottolineato che, nell'ambito dei servizi *online*, sembra prevalere l'orientamento per cui all'interessato viene chiesto di esprimere un consenso basato non su un'informativa completa, relativa ai diversi aspetti del trattamento, bensì su un'informativa che si limita a indicare le misure adottate per garantire la sicurezza dei dati. Tale tendenza appare del resto in linea con la recente adozione, ispirata al principio della "*privacy by design*", di misure di protezione direttamente inserite nell'ambito delle diverse tecnologie in uso (soprattutto per quanto riguarda Internet, ovvero di sistemi di *cd.* "*privacy default setting*", impostazioni orientate sin dall'inizio al rispetto delle regole di

protezione dati). In tale contesto, il ruolo delle autorità di protezione dati dovrà estendersi alla individuazione di misure di sicurezza e modalità *standard* di erogazione di servizi idonee a garantire un'elevata tutela dei diritti degli utenti.

Nella sezione riservata alle sole autorità di protezione dei dati accreditate, sono state discusse le risoluzioni ed i *report* sottoposti alla Conferenza per l'adozione, nonché i risultati di un'indagine focalizzata sulle esperienze delle autorità nazionali, con specifico riferimento ai rapporti (di collaborazione e/o conflitto) con altre autorità di regolazione. È stato deciso di ammettere come membro della Conferenza la *Federal Trade Commission* statunitense e le autorità di protezione dati della Repubblica moldava, di Albania, Bulgaria, Messico nonché, senza diritto di voto, l'Autorità comune di controllo (*Joint Supervisory Body*) di EUROJUST. Sono state adottate nuove regole di accreditamento alla Conferenza ed è stata decisa l'istituzione di un comitato esecutivo ad *interim* per proseguire il lavoro intrapreso affinché la Conferenza stessa assuma una più stabile struttura organizzativa.

La Conferenza si è conclusa con l'adozione, in particolare, di una risoluzione promossa dall'Autorità francese di protezione dati, con la quale si chiede la convocazione di una conferenza intergovernativa per adottare i princìpi internazionali in materia di *privacy* approvati a Madrid lo scorso anno. È stata altresì adottata la risoluzione, promossa dall'Autorità canadese, sulla "*privacy by design*", presentata come una vera e propria impostazione di carattere generale, da includere nella configurazione e nella gestione delle tecnologie e dei sistemi dell'informazione. Al riguardo sono stati individuati alcuni princìpi fondamentali, quali la necessità di un atteggiamento preventivo e non "rimediale" rispetto alla protezione dei dati, l'introduzione di impostazioni *pro privacy* incorporate nel *design* delle tecnologie adoperate, la visibilità e la trasparenza, il rispetto per la *privacy* dell'utente.

La risoluzione si conclude con un invito alle autorità di protezione dei dati a fornire un contributo attivo nella diffusione della "*privacy by design*", in particolare attraverso apposite campagne di sensibilizzazione, al fine di incoraggiare la ricerca su tali tecniche e promuovere l'introduzione di tale concetto nella formulazione delle *privacy policy* e della relativa normativa.

Spring Conference 2010

Il 29 e 30 aprile si è svolta la consueta Conferenza di primavera dei garanti europei della protezione dei dati, quest'anno ospitata dall'Autorità ceca a Praga.

La Conferenza, che sin dal titolo ha sottolineato l'intenzione di "guardare al futuro, soppesando il passato", si è aperta con una sessione dedicata al tema "Internet delle cose" ("*Internet of things*") ed alla costante tracciabilità degli interessati, derivante dall'utilizzo delle nuove tecnologie.

Nella seconda sessione, dedicata ai minori ed alle reti sociali, diverse autorità hanno illustrato le attività intraprese per meglio comunicare con gli utenti più giovani sviluppando linguaggi accessibili ed efficaci.

Il tema centrale, affrontato nel corso della sessione presieduta dal Presidente del Gruppo Art. 29, è stato la protezione dei dati personali nel contesto attuale, nel quale tali diritti sono normativamente rafforzati (anche in virtù del riconoscimento come diritti fondamentali ai sensi del Trattato di Lisbona) ma, al contempo, sono di fatto affievoliti dalle criticità determinate dal "dominio" di soggetti internazionali e dai mutamenti tecnologici. Una particolare riflessione ha riguardato il ruolo del settore pubblico rispetto al trattamento dei dati. Il Presidente del Garante ha introdotto il tema del rapporto tra diritto di accesso e diritto alla riservatezza facendo riferimento ai diversi modelli di amministrazione e ai diversi gradi di trasparenza che possono accompagnare lo svolgimento di attività pubbliche.

Un *panel* specifico è stato poi dedicato alla profilazione su base etnica ed ai punti di contrasto con i princìpi di protezione dei dati personali.

Nel corso della Conferenza le autorità hanno accolto la richiesta di partecipazione presentata dall'Autorità di protezione dati albanese ed hanno preso atto della sussistenza di richieste analoghe, che saranno valutate in occasione della prossima conferenza, da parte della competenti autorità di Bosnia Erzegovina e Moldavia.

La Conferenza ha adottato quattro risoluzioni. La prima, sul futuro della protezione dei dati e della *privacy*, richiama i princìpi fondamentali in materia e chiede un'attenzione particolare agli effetti della globalizzazione e delle nuove tecnologie su tali diritti. La risoluzione, nel prendere atto del crescente ricorso –per finalità di contrasto del terrorismo

e di altri fenomeni di criminalità– a dati raccolti originariamente per finalità diverse, conferma la necessità che i titolari verifichino che i trattamenti siano basati sul consenso, laddove legittimo, e avvengano in conformità a quanto previsto da basi legali idonee, nonché alle condizioni rigorose poste dal legislatore per regolare l'"uso secondario" dei dati. La risoluzione chiede anche che ogni iniziativa legislativa e l'introduzione di nuove tecnologie sia preventivamente sottoposta ad una valutazione di impatto sulla *privacy* ed accompagnata da misure di "*privacy by design*" che riducano il più possibile l'interferenza sulla *privacy*.

La Conferenza ha altresì rinnovato la richiesta di stabilire un corpo omogeneo di regole e *standard* internazionali –che includa i trattamenti di dati per finalità di polizia e giustizia– richiamando quelli adottati a Madrid nella Conferenza internazionale del 2009 e la Convenzione del Consiglio d'Europa.

Altre due risoluzioni hanno riguardato l'uso dei "*body scanner*" negli aeroporti, evidenziando l'esigenza di rispettare i princìpi di necessità e proporzionalità, anche con riferimento al possibile negoziato per concludere un accordo sulla protezione dei dati tra Unione europea e Stati Uniti.

Un'altra risoluzione indica la necessità di azioni comuni, a livello europeo ed internazionale, per educare e rendere consapevoli le nuove generazioni. La risoluzione invita le autorità di protezione dei dati, anche attraverso azioni coordinate, a sviluppare strumenti idonei a proteggere la *privacy* dei giovani e a stimolare l'adozione da parte dei titolari del trattamento di "*privacy policy*" semplici e comprensibili. Sono state inoltre incoraggiate le azioni dei governi dirette ad adottare iniziative specifiche per rafforzare la tutela dei giovani, anche tramite campagne di informazione e di educazione.

Nell'ambito dei lavori dedicati all'attività svolta dal Gruppo di lavoro polizia e giustizia (*Working Party on Police and Justice - WPPJ*; v. *infra*) la *Spring Conference* ha approvato, dopo la presentazione svolta da Francesco Pizzetti, presidente del *WPPJ*, i documenti presentati, ed in particolare il Rapporto annuale di attività per l'anno 2009, il progetto di raccomandazioni in materia di misure attuative della Convenzione sulla criminalità informatica del Consiglio d'Europa, il progetto di decisione relativa ad una politica coordinata

di controllo (attuativa del "manuale" approvato nel corso della precedente Conferenza di primavera), il progetto di decisione relativa all'inserimento di una clausola *standard* di protezione dati negli accordi bilaterali con Paesi extraeuropei in materia di "*law enforcement*", la bozza di risoluzione proposta dall'Autorità di protezione dati tedesca a complemento del lavoro svolto dal *WPPJ* (e dal Gruppo Art. 29) con la predisposizione delle osservazioni per la consultazione aperta dalla Commissione europea sul possibile contenuto di un accordo Unione europea - Stati Uniti sui princìpi in materia di trattamento dei dati personali.

20.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

Il Gruppo Art. 29, mantenendo il suo ruolo di stimolo e di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha attivamente contribuito al dibattito in materia di valutazione dell'attualità della Direttiva n. 95/46/CE e ai lavori preparatori per la possibile revisione della stessa.

Più in generale, il Gruppo ha analizzato sia il quadro giuridico vigente –per un'applicazione più coerente e corretta dei princìpi di protezione dei dati– sia le nuove sfide connesse allo sviluppo tecnologico, alla globalizzazione e al mutato scenario istituzionale dell'Unione europea conseguente all'entrata in vigore del Trattato di Lisbona.

Tale impegno risulta dal programma di lavoro 2010-2011 (WP 170), che si articola secondo quattro direttive fondamentali: 1) assicurare la corretta applicazione del quadro giuridico vigente e preparare quello futuro (attraverso l'interpretazione delle disposizioni chiave della Direttiva n. 95/46/CE, l'attuazione della direttiva e-*privacy*, recentemente modificata dalla Direttiva n. 2009/136/CE, la valutazione delle conseguenze dell'entrata in vigore del Trattato di Lisbona); 2) affrontare la globalizzazione intervenendo sulla disciplina relativa ai flussi transfrontalieri di dati personali, ovvero sulle "norme vincolanti d'impresa" ("*binding corporate rules*"), sull'attuazione degli accordi di "approdo sicuro" ("*Safe Harbor*"), nonché sulla valutazione di adeguatezza dei Paesi terzi e partecipando ai lavori sulla standardizzazione; 3) rispondere alle *cd.* "sfide tecnologiche", dedicando particolare attenzione alle tematiche del "*cloud computing*", dei "motori di ricerca" (in

particolare, le garanzie del "diritto all'oblio" rispetto all'utilizzo dei sistemi di ricerca *online*) dei servizi di *social network*; 4) migliorare l'efficacia dell'azione di *enforcement* del Gruppo Art. 29 e delle autorità per la protezione dei dati, sviluppando i metodi d'indagine delle autorità nazionali e promuovendo strumenti e forme di cooperazione tra di esse.

Nell'affrontare i molteplici impegni evidenziati, ivi compresa l'interpretazione del diritto vigente, particolare attenzione è stata dedicata al concetto di legge applicabile. In merito è stato adottato il parere WP 179 del 16 dicembre 2010 (v. *infra*) che ha affrontato i principali problemi interpretativi posti dai criteri di territorialità previsti dalla Direttiva n. 95/46/CE, soprattutto con riferimento a situazioni in cui l'attività di trattamento dei dati sia effettuata nel territorio di più Stati membri. Tale lavoro si è basato sull'attività di approfondimento intrapresa nel corso del 2009, conclusasi nel febbraio 2010 con l'adozione di un importante e documentato parere (WP 169 del 16 febbraio 2010, v. *infra*).

Sempre con riferimento all'interpretazione della Direttiva n. 95/46/CE, il Gruppo ha altresì iniziato ad esaminare il tema del "consenso" dell'interessato nel sistema delle garanzie per la protezione dei dati, per precisare fino a che punto lo stesso possa legittimare al trattamento dei dati personali, tenendo anche conto dei servizi di comunicazione elettronica, caratterizzati da asimmetrie informative tra operatori economici e utenti e dalle difficoltà pratiche legate alla manifestazione del consenso *online*.

In merito all'attività volta alla revisione della direttiva ed all'individuazione delle sfide poste dal mutato scenario istituzionale e tecnologico, hanno costituito oggetto di particolare attenzione da parte del Gruppo Art. 29 i seguenti aspetti, già rappresentati in sintesi nel "*Contributo alla consultazione pubblica sul futuro della protezione dati*" WP 168 del 1° dicembre 2009 (v. *Relazione* 2009, p. 264): 1) la disciplina delle categorie particolari di dati (*cd.* "dati sensibili"); 2) il sistema di notificazione, delineato dall'art. 18 della direttiva, soprattutto per una possibile semplificazione; 3) le forme di cooperazione tra le autorità di protezione dei dati, previste dall'art. 28, par. 6, della direttiva.

Del parere del Gruppo Art. 29 sui temi fin qui richiamati terrà conto la Commissione europea nell'elaborazione della proposta di revisione della Direttiva n. 95/46/CE, prevista entro la fine del primo semestre del 2011.

In proposito si rileva, da un lato, che per quanto concerne la semplificazione degli oneri di notificazione, l'individuazione di un denominatore comune tra le posizioni espresse dalle autorità nazionali dovrebbe consentire di pervenire all'adozione del relativo parere nel corso della prima parte del 2011, dall'altro, che il tema della cooperazione tra autorità nazionali di protezione dei dati, soprattutto nella prospettiva di individuare strumenti di coordinamento e di collaborazione in relazione alle tematiche di rilevanza transnazionale o alle ipotesi in cui giurisdizione e legge applicabile non coincidano, presenta non poche criticità (prima tra tutte, i diversi poteri, anche sanzionatori, delle suddette autorità).

Con riferimento all'attività di *Google* sul territorio di diversi Stati membri nell'ambito del servizio "*Street View*", il lavoro svolto attraverso il coordinamento delle posizioni e delle azioni delle autorità nazionali nell'ambito del Gruppo Art. 29, ha costituito un emblematico esempio di efficace cooperazione tra autorità nazionali di protezione dati. Infatti, la circostanza che le operazioni di raccolta e trattamento dei dati effettuate da *Google* siano state indagate e valutate da parte di più autorità nazionali ha reso sicuramente opportuno l'intervento del Gruppo Art. 29 nell'attività di *enforcement*, pur nel rispetto delle specificità dei singoli casi e delle normative nazionali applicabili. Allo scopo di coordinare e uniformare le risposte alle eventuali violazioni della *privacy*, il Gruppo Art. 29 ha raccolto dalle singole autorità nazionali informazioni relative alle esperienze di monitoraggio, ed ha posto in essere un'analisi congiunta per comprendere la natura e la tipologia dei dati raccolti e trattati da *Google*, soprattutto con riferimento alle possibilità di controllo continuo delle reti *Wi Fi* effettuato nel corso della raccolta di immagini per il servizio *Street View*.

È altresì stata sottolineata l'importanza delle problematiche connesse all'uso delle tecnologie informatiche, soprattutto in relazione all'utilizzo di reti *wireless* o sistemi *GPS*, in grado di localizzare la posizione dell'individuo e monitorarne gli spostamenti.

Dopo una accurata analisi è stato adottato dal Gruppo Art. 29 un parere dedicato alla *cd.* "pubblicità comportamentale", quale forma invasiva di *marketing* fondato sulla profilazione degli utenti in rete. A questo ha fatto seguito un'attività di consultazione dei principali operatori del settore, in merito agli aspetti tecnici richiamati nel documento succitato (*Parere*

2/2010 sulla pubblicità comportamentale *online* - WP 171, v. *infra*; "*Letter from the Article 29 Working Party addressed to the Ad Network Providers*" e "*Letter from the Article 29 Working Party addressed to the Browser Providers*", entrambe del 29 ottobre 2010, v. *infra*).

Sempre con particolare attenzione al settore degli scambi di dati in un contesto dal carattere marcatamente commerciale, sono state approfondite le tematiche legate ai flussi transfrontalieri di informazioni, sia attraverso la semplificazione del sistema di adozione delle "norme vincolanti d'impresa" ("*binding corporate rules*") ad uso delle società di carattere multinazionale, sia tramite l'estensione della platea dei Paesi terzi considerati adeguati (WP 177 in merito all'adeguatezza dell'Uruguay, v. *infra*).

La crescente importanza della circolazione dei dati personali nell'ambito del mercato globalizzato, inoltre, ha indotto il Gruppo ad esaminare il concetto di "*accountability*" (inteso come regola complessiva di responsabilità ed impegno assunta dal titolare del trattamento, che permea l'intera organizzazione aziendale al rispetto dei princìpi di protezione dei dati) e ad esprimersi in modo favorevole all'introduzione di tale principio nel nuovo quadro giuridico europeo di protezione dei dati, con il parere del 13 luglio 2010 (WP 173, v. *infra*).

Il Gruppo ha poi continuato ad occuparsi del trasferimento e trattamento di dati finanziari, soprattutto in relazione al perdurante accesso del "*US Department of Treasury*" ai dati contenuti nel *database* di *Swift*. Per consentire l'accesso a questi dati da parte degli Stati Uniti è stato infatti negoziato dalla Commissione un accordo sulla trasmissione dei dati di messaggistica finanziaria tra Unione europea e Stati Uniti, direttamente vincolante per gli Stati membri dell'UE a partire dal 1° agosto 2010 (Accordo *cd.* "*TFTP2*" –"*Terrorist Finance Tracking Program*"– di cui alla Decisione del Consiglio del 13 luglio 2010, pubblicata nella *G.U.U.E.* L 195 del 27 luglio 2010).

Parimenti approfondito è stato l'esame, anche con rappresentanti del settore finanziario e della Direzione generale mercato interno della Commissione europea, dell'impatto, in materia di protezione dei dati, delle direttive antiriciclaggio e per la prevenzione del finanziamento del terrorismo, in particolare con riferimento all'applicazione della normativa nazionale di recepimento.

Continua e costante attenzione è stata mantenuta riguardo al trattamento dei dati dei passeggeri in relazione all'obbligo per i vettori aerei di fornire in anticipo, e a pena di sanzioni, dati di prenotazione ed altri dati identificativi del passeggero alle autorità competenti dei Paesi di destinazione. Sono in corso di rinegoziazione, da parte della Commissione, accordi al fine di regolare l'uso di tali dati da parte, al momento, degli Stati Uniti, del Canada e dell'Australia.

Il Gruppo Art. 29 ha valutato l'approccio generale da seguire per la salvaguardia dei requisiti posti dalla legislazione in materia di protezione dei dati personali nella negoziazione di tali accordi (Parere 7/2010 sulla comunicazione della Commissione europea sull'approccio globale ai trasferimenti di dati *PNR* verso Paesi terzi (WP 178, v. *infra*), formulando considerazioni anche con riferimento alla possibile adozione di un sistema di trattamento dei dati "*Passenger Name Records*" (*PNR*) europeo, nonché con riferimento al programma "*Electronic System for Travel Authorization*" (*ESTA*) adottato dagli Stati Uniti ed alla possibile adozione di un sistema *ESTA* europeo.

Sul lato *enforcement* l'Autorità ha coordinato, in qualità di *rapporteur*, l'azione comune sull'applicazione della direttiva europea in materia di conservazione dei dati di comunicazione elettronica a fini di prevenzione e contrasto della criminalità (Direttiva n. 2006/24/CE, *cd.* "*direttiva Frattini*") ed ha redatto la sintesi e le raccomandazioni per la valutazione del Gruppo.

Il Gruppo Art. 29 ha adottato il *report* nella forma di parere (*Report 01/2010 on the second joint enforcement action* - WP 172 del 13 luglio 2010, v. *infra*) e lo ha presentato pubblicamente, anche in occasione della Conferenza del 3 dicembre 2010, organizzata dalla Commissione europea per analizzare in dettaglio i punti fondamentali della direttiva.

Il lavoro, che ha evidenziato la non uniforme, e talvolta anche non corretta, applicazione delle disposizioni della direttiva "*data retention*" da parte degli Stati membri, ha determinato forti prese di posizione da parte delle autorità di protezione dati in merito alla necessità di modifiche della stessa, anche alla luce delle sentenze adottate dalle corti costituzionali di diversi Paesi, e non mancherà di influenzare il Rapporto che la Commissione deve presentare sull'applicazione della direttiva.

Infine, sono stati istituiti nuovi gruppi di lavoro o ricostituiti sottogruppi che avevano già svolto i compiti originariamente previsti dai rispettivi mandati. È il caso specifico del gruppo "*Health data*", del sottogruppo "*e-Government*" e del gruppo di lavoro "*Biometrics*".

Al primo è stato attribuito lo studio dell'impatto *privacy* del progetto "*European Patient Smart Open Services*" (*epSOS*), relativo alla trasmissione dei dati sanitari concernenti uno stesso paziente tra Stati membri dell'Unione europea, con il principale compito di esaminare la normativa e la prassi degli Stati membri che prevedono la registrazione elettronica di dati sanitari.

Al sottogruppo "*e-Government*" è stato dato mandato di analizzare gli aspetti di protezione dei dati personali legati al progetto *STORK*, volto a creare una piattaforma interattiva per lo scambio di informazioni relative all'identità dei cittadini con prevalente applicazione nel settore dell'*e-Government*. Il programma dovrebbe consentire l'accesso *online*, mediante semplice presentazione delle credenziali identificative del soggetto (*cd.* "*eID*"), a servizi per lo più di carattere amministrativo, in tutta l'Unione europea.

Infine, al gruppo "*Biometrics*" spetterà il compito di procedere all'aggiornamento del documento di lavoro sulla biometria (WP 80), adottato dal Gruppo il 1° agosto 2003, anche in considerazione del crescente utilizzo dei dati biometrici negli Stati membri, da parte di operatori sia pubblici che privati.

Di alcuni dei pareri e documenti citati in questo paragrafo si dà di seguito un sintetico resoconto, raggruppandoli in base ai temi trattati:

a. Interpretazione della Direttiva n. 95/46/CE

Parere 1/2010 sui concetti di titolare e responsabile (WP 169)

Il Gruppo ha analizzato la definizione di "titolare" ("*data controller*") del trattamento dei dati, e la sua interazione col soggetto responsabile ("*data processor*"), figure centrali nell'applicazione della Direttiva n. 95/46/CE (per ciò che riguarda l'individuazione del soggetto che risponde dell'osservanza delle norme di protezione dei dati, la determinazione della legge applicabile, l'individuazione del soggetto di fronte al quale gli interessati possono esercitare i loro diritti). Il parere non tiene conto della terza figura soggettiva (l'incaricato) prevista dalla normativa italiana, la cui individuazione non ha fino ad ora posto particolari problematiche, trattandosi

del soggetto che materialmente pone in essere le operazioni di trattamento su istruzione del titolare o del responsabile, ove nominato. L'approccio utilizzato è di carattere funzionale, ovvero orientato ad un'analisi dei diversi ruoli soggettivi che intervengono nell'attività di trattamento con maggiore o minore responsabilità a seconda del grado di influenza di questi sulle decisioni inerenti le attività di trattamento medesime. È stata innanzitutto approfondita la figura del "titolare" con riguardo a profili diversi, quali la componente soggettiva; la possibilità di una responsabilità plurima, nonché le differenze con le altre figure che intervengono nel trattamento. Con riguardo alla figura del "responsabile", sono stati evidenziati gli aspetti legati alla "nomina" da parte del titolare, soprattutto con riferimento alle ipotesi, in crescente aumento, di deleghe "multilivello o estese" proprie delle strutture organizzative complesse. In questo contesto, il documento ha affrontato i diversi scenari in cui si prevede l'intervento di titolari e responsabili del trattamento, da soli o congiuntamente con altri, con vari gradi d'autonomia e di responsabilità, sottolineando l'esigenza di attribuire le responsabilità in modo da garantire un'adeguata osservanza delle norme in materia di protezione dei dati.

Parere 8/2010 sul diritto applicabile (WP 179)

Il testo, nell'illustrare i principali problemi applicativi connessi all'art. 4 della Direttiva n. 95/46/CE, ha individuato alcune possibili soluzioni anche pratiche dei casi più complessi di conflitti tra leggi astrattamente applicabili. Sono stati quindi analizzati i diversi criteri di collegamento della direttiva. In particolare è stata chiarita la portata effettiva del principio di stabilimento, nonché l'interpretazione da fornire al "grado di coinvolgimento" dello stabilimento situato nel territorio di uno Stato membro rispetto all'attività di trattamento posta in essere dal titolare ed al concetto di "strumenti situati sul territorio di uno Stato membro". Infine sono state proposte alcune possibili soluzioni, sia con riferimento al caso in cui il titolare disponga di stabilimenti situati in diversi Stati membri dell'Unione europea (suggerendo l'utilizzo del criterio dello stabilimento "principale" del titolare del trattamento, accompagnato dall'auspicata armonizzazione delle legislazioni nazionali di protezione dei dati), sia nell'ipotesi di titolare stabilito in un Paese terzo. In quest'ultimo

caso, è stato proposto di ricorrere innanzitutto al criterio del *cd.* "*targeting*", che consiste nell'individuazione dell'ambito dei destinatari potenziali per le attività di trattamento poste in essere dal titolare (ad es., servizi forniti solo a soggetti residenti nell'UE; informazioni fornite solo nelle lingue dell'UE) e, in via residuale, al criterio di collegamento rappresentato dagli "strumenti situati nel territorio dello Stato" (*cd.* "*means*"), già previsto dal vigente testo della direttiva;

b. Accountability

Parere 3/2010 sul principio di responsabilità (WP 173)

Il parere è principalmente volto a contribuire al processo di revisione della Direttiva n. 95/46/CE, rafforzando il ruolo del titolare del trattamento, anche mediante una sua maggiore responsabilizzazione, nel garantire il rispetto delle regole di protezione dei dati. Il nuovo approccio si propone di creare specifiche responsabilità in capo al titolare in ordine all'attuazione della normativa in materia di *privacy*, differenziando gli obblighi di diligenza (e conseguentemente gli adempimenti) in base al rischio effettivo del trattamento. Più nello specifico, il parere si sofferma sui due elementi fondamentali di cui il principio di *accountability* dovrebbe comporsi:

- il rispetto da parte di tutti i titolari del trattamento di uno *standard* minimo di protezione dei dati (in particolare, attraverso l'attuazione di "*privacy policy*" interne, l'istituzione di "*privacy officers*" e di sistemi di formazione del personale dipendente) e di meccanismi di verifica della loro efficacia (*audit* interni ed esterni);
- la possibilità, su base volontaria, in capo al titolare, di rispettare *standard* di protezione che vadano oltre i parametri minimi individuati dalla legge (ad es., determinazione di tempistiche più brevi di riscontro alle istanze di accesso degli interessati; adozione di misure di sicurezza più stringenti rispetto ai parametri minimi fissati dalla legge, ecc.).

Un ruolo di fondamentale importanza, infine, dovrebbe essere riconosciuto alle autorità di protezione dei dati personali sia in relazione all'individuazione dei parametri da rispettare (anche nella prospettiva di individuare sistemi di certificazione dell'*accountability*), sia in ordine ai sistemi di controllo e di verifica (con il possibile potenziamento dei relativi poteri sanzionatori);

c. Pubblicità comportamentale e protezione dei dati personali *online*

Parere 2/2010 sulla pubblicità comportamentale *online* (WP 171)

Il Gruppo si è pronunciato sulle garanzie specifiche da applicare al settore della pubblicità comportamentale su Internet. Si tratta, in particolare, di forme di *marketing* che prevedono il tracciamento degli utenti durante la navigazione in rete e la creazione di profili, poi utilizzati per messaggi pubblicitari personalizzati. Nel parere si sottolinea innanzitutto che i fornitori di reti pubblicitarie, ai sensi dell'art. 5, par. 3, della direttiva e-*privacy* (Direttiva n. 2002/58/CE, recentemente modificata dalla Direttiva n. 2009/136/CE), possono collocare marcatori (*cookie*) o dispositivi analoghi nelle apparecchiature terminali degli utenti e raccogliere informazioni tramite tali dispositivi soltanto con il previo consenso informato degli utenti. Oltre a stabilire l'obbligo di introduzione di meccanismi di "*opt in*" preliminare che assicurino l'accettazione, da parte dell'interessato, del monitoraggio del comportamento di navigazione ai fini dell'invio di pubblicità personalizzata, il parere fornisce indicazioni sul generale obbligo di trasparenza in relazione agli scopi ed alle modalità del trattamento, ai diritti degli interessati (tra l'altro, accesso, rettifica e cancellazione dei dati) ed ai corrispondenti obblighi per editori e fornitori di reti pubblicitarie. Il Gruppo, tramite le autorità nazionali, ha poi avviato la consultazione delle parti interessate, in particolar modo fornitori di reti pubblicitarie e fornitori di *browser* sui profili tecnici, con lettere il cui testo è disponibile sul sito *web* del Gruppo Art. 29.

Parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel *marketing* diretto (WP 174)

L'associazione europea di operatori di *marketing FEDMA* ("*Federation of European Direct and Interactive Marketing*") ha predisposto una bozza di codice di condotta, relativa all'utilizzo dei dati personali per le attività di *cd.* "*marketing online*", sottoponendola al Gruppo Art. 29 per una pronuncia ai sensi dell'art. 27 della Direttiva n. 95/46/CE. La messa a punto del testo è stata alquanto complessa, avendo richiesto oltre quattro anni di lavoro, in contraddittorio con il sottogruppo appositamente costituito in seno al Gruppo Art. 29. In considerazione delle modifiche da ultimo apportate da *FEDMA* al codice di condotta, in conformità alle prescrizioni indicate nel parere WP 171 del 2010 sulla pubblicità comportamentale *online*, nonché alla Direttiva n. 2002/58/CE come recentemente modificata, il Gruppo

Art. 29 ha espresso, il 13 luglio 2010, parere favorevole sulla compatibilità del codice di condotta europeo con i princìpi e le norme in materia di protezione dei dati personali;

d. Decisioni di adeguatezza di Paesi terzi

Parere 6/2010 sul livello di protezione dei dati personali nella Repubblica orientale dell'Uruguay (WP 177)

Su richiesta della Commissione europea, il Gruppo Art. 29 ha valutato il livello di protezione dei dati esistente in Uruguay, giungendo ad un giudizio di adeguatezza ai sensi dell'art. 25, comma 6, della Direttiva n. 95/46/CE che consente il trasferimento di dati personali dall'Unione europea. In particolare, è stato rilevato un impianto normativo che si ispira a quello introdotto dalla direttiva, con particolare riferimento all'ambito di applicazione (la legge in materia di protezione dei dati si applica sia al settore pubblico sia a quello privato), alle modalità del trattamento ed ai requisiti di qualità dei dati;

e. Clausole contrattuali *standard*

FAQ sulle clausole contrattuali *standard* (WP 176)

In materia di "*standard contractual clauses*" sono state adottate alcune "*frequently asked questions*" (*FAQ*) dedicate all'attuazione della Decisione 2010/87 della Commissione ed in particolare al nuovo *set* di clausole "*controller to processor*". Il testo, con lo scopo primario di garantire maggiore armonizzazione nel recepimento della decisione da parte delle autorità nazionali ed un'applicazione uniforme delle clausole da parte dei titolari del trattamento, si propone di chiarire alcune specifiche problematiche, soprattutto con riferimento ai trasferimenti di dati da *controller* a *processor* stabilito nell'Unione europea, con *subprocessor* stabilito in un Paese terzo. Sono state inoltre esaminate alcune criticità interpretative, in particolare in materia di designazione del *subresponsabile*, di utilizzo di un unico contratto da parte di un responsabile che affidi il trattamento al medesimo *subresponsabile* per conto di differenti titolari, di adozione delle clausole a prescindere dalla effettiva designazione di *subresponsabili*, dell'obbligo di deposito/notifica delle clausole contrattuali tipo alle autorità di protezione dati.

f. Trasferimenti di dati UE-Stati Uniti a fini di cooperazione giudiziaria e di polizia, per il contrasto del terrorismo e di reati gravi

Accordo quadro UE-USA in materia di protezione dati: lettera del Gruppo Art. 29

Con riferimento al *cd.* "accordo quadro" ("*umbrella agreement*") tra Unione europea e Stati Uniti sulla protezione dei dati personali, il Gruppo Art. 29 il 19 novembre 2010, con un parere in forma di lettera ha precisato che l'accordo dovrebbe rappresentare una cornice comune di requisiti per la protezione dei dati personali, per tutti i trattamenti diretti al contrasto delle attività criminali (inclusi i trattamenti aventi ad oggetto dati provenienti da soggetti privati). Il Gruppo, inoltre, ha criticato la clausola dell'accordo che pone l'eccezione relativa ai trattamenti di dati per scopi di "sicurezza nazionale" (trattamenti per i quali viene così esclusa l'applicabilità dalle regole generali previste dall'accordo quadro), auspicandone una riformulazione che eviti la possibilità di interpretazioni estensive. Per quanto concerne il rapporto dell'accordo quadro con quelli già in vigore tra Stati Uniti e Unione europea e Stati membri ("accordi settoriali"), il Gruppo ha proposto l'applicazione retroattiva dall'accordo quadro agli accordi esistenti unitamente, in certi casi, ad un regime transitorio della durata massima di 3 anni. Sono stati inoltre rilevati altri punti critici quali: il rispetto dei diritti contemplati dalla Direttiva n. 95/46/CE, dalla Decisione-quadro 2008/977/GAI e dalle relative disposizioni nazionali di recepimento; la previsione di una clausola ostativa al trasferimento dei dati personali nei casi in cui sia prevista l'applicazione della pena di morte; l'effettiva garanzia dei diritti degli interessati (accesso, rettifica, cancellazione), tenendo conto del ruolo e delle funzioni delle autorità di protezione dati nazionali; il diritto degli interessati a ricorrere in via amministrativa e giurisdizionale avverso le decisioni relative al trattamento che li riguardino; il divieto di trasferimenti di tipo "massivo"; le condizioni e i limiti per il trasferimento ulteriore dei dati; i tempi di conservazione dei dati, adeguati e proporzionali alle finalità pubbliche perseguite; la durata limitata nel tempo dell'accordo e le possibilità di proroga, controllo e revisione congiunta dello stesso, da effettuarsi previo esame da parte della delegazione comune ("*joint review team*"), nella quale siano rappresentate le autorità di protezione dati nazionali.

Accordo sul trasferimento di dati finanziari: lettere del Gruppo Art. 29

Per quanto concerne i trasferimenti transatlantici di dati finanziari, si segnala l'intensa attività svolta dal Gruppo Art. 29, e dal sottogruppo "*Financial Matters*", in merito all'accordo tra Unione europea e Stati Uniti sulla trasmissione dei dati di messaggistica

finanziaria. Per rendere più effettiva la protezione dei dati personali nell'ambito dell'accordo, il Gruppo Art. 29, congiuntamente al Gruppo di lavoro polizia e giustizia (*WPPJ*), ha adottato il parere in forma di lettera del 27 gennaio 2010, sull'accordo "ponte" ("*Interim Agreement*"), e il parere del 25 giugno 2010, sempre in forma di lettera, sulla bozza dell'accordo "*TFTP2*". Con quest'ultima lettera, in special modo, è stata sottolineata l'importanza che l'accordo non limiti i poteri di intervento delle autorità nazionali per la protezione dati e garantisca l'effettività dei diritti degli interessati. Sempre con riferimento all'accordo tra UE e Stati Uniti per la trasmissione ed il trattamento di dati finanziari *TFTP* (*Swift*), in data 5 agosto 2010 il Gruppo ha inviato al Commissario responsabile per gli Affari interni la lettera sulla partecipazione delle autorità di protezione dati alla procedura per la revisione ed il controllo dell'attuazione dell'accordo ("*joint review mechanism*"). Essa indica le autorità del Belgio e dei Paesi Bassi come rappresentanti delle autorità nazionali di protezione dati nella delegazione dell'Unione europea per la revisione dell'accordo ("*European Union review delegation*") ed evidenzia alcune criticità concernenti, in particolare, il ruolo di EUROPOL, di cui non sono chiari i poteri e l'esercizio delle funzioni di controllo al momento dell'approvazione delle richieste di dati da parte del Dipartimento del tesoro degli Stati Uniti. Le autorità dichiarano inoltre di volere esercitare, con la necessaria indipendenza e con pieni poteri, il proprio ruolo di supervisione del rispetto delle garanzie previste dall'accordo *TFTP* in termini di protezione dati. I testi delle lettere sono disponibili sul sito *web* del Gruppo.

g. Dati dei passeggeri aerei e accordi *PNR*

Parere 7/2010 sulla comunicazione della Commissione europea sull'approccio globale ai trasferimenti dei dati *PNR* verso Paesi terzi (WP 178)

Il Gruppo ha espresso la propria posizione in merito alla Comunicazione del 21 settembre 2010 della Commissione europea sull'approccio globale ai trasferimenti dei dati *PNR* verso Paesi terzi (COM(2010) 492). Il Gruppo, pur apprezzando l'iniziativa, volta a definire misure minime di salvaguardia per la protezione dei dati personali, ha manifestato perplessità in merito alla necessità e proporzionalità di tale trattamento per finalità di "*law enforcement*" nel contrasto alle attività di terrorismo. In particolare, si è evidenziato che lo scambio di dati *PNR* deve essere

considerato nel più ampio contesto del trattamento dei dati relativi ai passeggeri, che include, tra l'altro, anche i *cd.* "dati *API*" (*Air Passenger Information*), di cui alla Direttiva n. 2004/82/CE, i quali potrebbero, in alcuni casi, essere di per sé sufficienti a perseguire lo scopo di "*law enforcement*".

h. "*Enforcement*" sulla direttiva *data retention*

Rapporto 1/2010 sull'azione di *enforcement* (WP 172)

Il Gruppo, basandosi sui lavori del sottogruppo "*Enforcement*", di cui il Garante è stato *rapporteur*, ha approvato il 13 luglio 2010 il rapporto sull'azione di "*enforcement*" relativa alla direttiva *cd.* "*data retention*". Il rapporto è il risultato della valutazione, da parte delle autorità per la protezione dei dati personali, delle risposte ai questionari rivolti alle principali società attive nel settore delle comunicazioni elettroniche e degli esiti degli accertamenti condotti "sul posto" dalle autorità di protezione dati. È stata confermata, in particolare, l'esigenza di una migliore definizione del campo di applicazione della direttiva e del periodo di conservazione dei dati; nella specie riduzione del periodo "massimo" e introduzione di un termine "unico". È stata altresì ribadita la necessità di una trasmissione dei dati più sicura e preceduta da un'adeguata valutazione dei rischi specifici, nonché una definizione maggiormente armonizzata sia delle procedure per la comunicazione dei dati alle autorità competenti in materia di *law enforcement*, sia di alcuni concetti essenziali, ancorché ancorati al diritto nazionale, quali la nozione di "*serious crime*".

i. Protezione dati e tecnologie *RFID*

Privacy Impact Assessment RFID (WP 175 e WP 180)

Dopo un primo parere negativo del 13 luglio 2010 (WP 175) sulla prima proposta della *cd.* "*business community*" in materia di "*privacy impact assessment*" per le tecnologie *RFID* (applicazioni basate sull'identificazione a radiofrequenza), il Gruppo Art. 29 ha approvato la "*revised industry proposal*" l'11 febbraio 2011 (WP 180). In sostanza, in base al citato documento, gli operatori *RFID*, prima di utilizzare tali tecnologie, si impegnano a: 1) definire con chiarezza i fattori di rischio; 2) tener conto delle possibilità che le persone continuino a portare etichette *RFID* anche oltre l'area sorvegliata predefinita; 3) rispettare i princìpi per la disattivazione delle etichette *RFID* nel settore del commercio al dettaglio. Il processo di "*privacy impact*

assessment" (*PIA*) prevede, in particolare, una fase di pre-valutazione, per la classificazione delle tecnologie *RFID*, nonché una fase di valutazione dei rischi. Il Gruppo Art. 29 continuerà ad ogni modo i contatti con gli operatori economici interessati, anche al fine di valutare se la metodologia di *PIA* approvata dal Gruppo Art. 29 sia di fatto applicata dai produttori di *RFID*.

l. Protezione dati e tutela dei diritti di proprietà intellettuale

Lettera al Commissario Mr. Karel de Gucht sull'accordo anticontraffazione (*ACTA*)

Il Gruppo ha adottato il 15 luglio 2010 il parere in forma di lettera indirizzato al Commissario della Direzione generale commercio della Commissione europea, responsabile del negoziato dell'accordo *ACTA*, avente come principale obiettivo il contrasto delle violazioni dei diritti di proprietà intellettuale. Nel ricordare che le Parti contraenti hanno confermato, con dichiarazione congiunta del 16 Aprile 2010, l'esclusione dell'utilizzo del principio "*Three Strikes Out Scheme*" (ovvero la disconnessione da Internet dell'utente identificato per tre volte come autore di presunte violazioni del diritto di *copyright*), il Gruppo ha espresso contrarietà all'introduzione della "*Notice-and-Take-Down Procedure*" in base alla quale, nel caso di segnalazioni di violazioni del diritto di *copyright*, i fornitori di servizi *online* possono bloccare l'accesso ai contenuti scaricati dagli utenti, e sono tenuti a comunicare al titolare del diritto d'autore informazioni sull'identità del presunto autore della violazione. Infine, nelle conclusioni, ha sottolineato l'importanza di assicurare la tutela del *copyright* con misure necessarie e proporzionali, garantendo, al contempo, il diritto alla riservatezza delle parti coinvolte.

20.3. LA COOPERAZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Working Party on Police and Justice (*WPPJ*)

L'attività del *WPPJ* nel 2010 è proseguita sotto la presidenza italiana, secondo il programma di lavoro biennale adottato nel 2009, percorrendo due binari fondamentali. Da un lato, è stata mantenuta l'attenzione agli sviluppi normativi in sede europea con riguardo ai flussi di dati verso gli Stati Uniti ed altri Paesi extraeuropei per finalità giudiziarie e di polizia; dall'altro lato, è proseguita un'attività, concentrata su alcuni temi ritenuti di parti-

colare delicatezza, di monitoraggio degli sviluppi in materia di "terzo pilastro" a livello europeo, con riferimento al quadro normativo introdotto dal Trattato di Lisbona. Nel primo ambito di attività, occorre ricordare il contributo alla Consultazione pubblica della Commissione europea sul progetto di accordo (*cd.* "*accordo quadro*") tra Unione europea e Stati Uniti in materia di protezione dei dati personali e scambio di informazioni per finalità di polizia e giudiziarie, presentato congiuntamente al Gruppo Art. 29, i cui contenuti sono stati successivamente sintetizzati in una Risoluzione adottata dalla Conferenza di primavera delle autorità di protezione dati tenutasi a Praga. Il punto fondamentale è che l'accordo, commendevole in quanto volto a garantire un approccio uniforme, dovrà fissare un quadro di princìpi che troveranno applicazione in ogni futuro strumento convenzionale adottato in materia. L'accordo quadro non costituirà, pertanto, la base giuridica dei trattamenti in oggetto, che dovrà essere individuata di volta in volta nei modi opportuni e con riguardo alle specifiche circostanze. Il documento sottolinea, inoltre, alcune criticità del progetto di accordo: in particolare, le incertezze relative ai meccanismi di ricorso esperibili dai cittadini europei in caso di trattamenti illeciti svolti negli Stati Uniti ed all'esercizio dei diritti di accesso previsti dalla Direttiva n. 95/46/CE e dalle normative nazionali di recepimento. Nella Risoluzione della citata Conferenza di Primavera, le autorità europee di protezione dati hanno sottolineato anche la necessità di garantire un controllo indipendente sull'applicazione dell'accordo e degli strumenti attuativi. Sempre con riguardo ai flussi di dati Unione europea - Stati Uniti, il *WPPJ* ha commentato, congiuntamente con il Gruppo Art. 29, il nuovo testo dell'Accordo *TFTP* (*Terrorist Financial Tracking Program, TFTP2*), condividendone le numerose riserve ed evidenziando le ambiguità dell'articolato. Sul versante intraeuropeo, il *WPPJ* ha contribuito al dibattito sulla possibile revisione del quadro giuridico in materia di protezione dati alla luce del Trattato di Lisbona, in primo luogo in relazione all'incontro organizzato il 14 luglio con la Commissione europea ed alla presentazione di due documenti da parte della Commissione: il "*Piano di Azione*" per l'attuazione del Programma di Stoccolma (COM 2010/171, riguardante il potenziamento delle attività di cooperazione giudiziaria e di polizia); la "*Panoramica degli strumenti esistenti per la gestione delle informazioni nell'area di Libertà, Sicurezza Giustizia*" (COM 2010/385).

In tale occasione, il *WPPJ* ha confermato la propria visione della futura articolazione istituzionale, volta ad attuare le disposizioni di un quadro normativo unico ("*comprehensive legal framework*") che superi la precedente ripartizione delle politiche comunitarie in "Pilastri". Il contributo del *WPPJ* si è focalizzato sulla necessità di assicurare un ruolo di efficace supervisione alle autorità nazionali anche in settori sinora sottratti (almeno in parte) alla loro competenza e di mirare all'effettiva uniformità dei princìpi di protezione dati anche per quanto riguarda le attività di cooperazione giudiziaria e di polizia. In merito ai citati documenti della Commissione relativi al potenziamento della cooperazione giudiziaria e di polizia, il *WPPJ* ha adottato un "*Position Paper*", inviato alle istituzioni europee ed alle competenti autorità nazionali, per segnalare le incongruenze all'interno del "*Piano di Azione*" e sottolineare la necessità dell'immediato coinvolgimento delle autorità di protezione dati europee nell'attuazione della *policy* della Commissione nell'area del *cd.* "terzo pilastro". Il *WPPJ* ha altresì rilevato che l'obiettivo di assicurare il rispetto dei diritti fondamentali alla protezione dei dati ed alla *privacy*, così come proclamato nelle citate Comunicazioni della Commissione, deve essere garantito anche con riguardo alle banche dati ed agli strumenti attualmente esistenti. Nello sviluppo di nuovi strumenti occorrerà poi tenere conto dei princìpi di necessità e proporzionalità, e quindi dell'obbligo di documentare l'esigenza reale di raccogliere ed analizzare dati e informazioni per scopi di cooperazione giudiziaria e di polizia. Il *WPPJ* ha richiamato l'attenzione sul trattamento dei dati per attività di profilazione in relazione al rischio di discriminazione e di stigmatizzazione, nonché sulla prassi di stipulare, in determinati settori, accordi bilaterali *ad hoc* idonei a generare disomogeneità e incertezza del diritto. Il *WPPJ* ha inoltre avviato l'analisi dell'utilizzo dei dati genetici contenuti nelle banche dati nazionali (banche dati *DNA*) per finalità giudiziarie e di polizia, per verificare l'osservanza dei princìpi del "catalogo" (manuale) in materia di attività di supervisione e controllo elaborato dal *WPPJ* ed approvato dalla Spring Conference di Edinburgo nel 2009 (v. *Relazione* 2009, p. 273). A tal fine, il Gruppo ha predisposto un apposito questionario, di cui sta esaminando le risposte.

Il Gruppo ha poi monitorato la trasposizione a livello nazionale della decisione-quadro sulla protezione dati nel settore del terzo pilastro (Decisione 2008/977/GAI), valutando

lo "stato dell'arte" della disciplina del trattamento dei dati personali in ogni Stato membro e la prospettiva di uniformazione del quadro normativo.

Occorre, infine, fare riferimento al dibattito, apertosi nel corso del 2010 e proseguito nei primi mesi del 2011, sulla futura configurazione del rapporto fra *WPPJ* (che, si ricorda, è il gruppo di lavoro costituito dalla Conferenza di primavera e che riunisce le autorità di protezione dati europee, anche di Paesi non membri dell'Unione europea) e Gruppo Art. 29 (le cui competenze, prevalentemente connesse ai settore del *cd.* "primo pilastro", sono verosimilmente destinate ad ampliarsi in seguito alla revisione della Direttiva n. 95/46/CE secondo i princìpi introdotti dal Trattato di Lisbona). Si tratta di chiarire i termini della reciproca collaborazione tra i due Gruppi di lavoro onde evitare sovrapposizioni e garantire l'agevole transizione verso un sistema unitario di supervisione europeo in materia di protezione dei dati.

EUROPOL: l'attività dell'Autorità di controllo comune (ACC) e del comitato ricorsi

In relazione ad EUROPOL, fin dall'inizio del 2010, centrale è stata la discussione sulla definizione degli atti normativi necessari per assicurare la piena operatività della relativa Autorità di controllo comune nel mutato quadro giuridico (Decisione 2009/371/GAI del 6 aprile 2009, in vigore dal 1° gennaio 2010, che integra EUROPOL tra gli organismi dell'Unione europea).

La discussione si è focalizzata sull'organizzazione delle ispezioni nazionali e sul possibile coordinamento delle stesse, eventualmente sulla base del modus operandi approvato dal Gruppo di lavoro polizia e giustizia. Al riguardo, si è chiarito che il termine "ispezione" fa riferimento a due diverse attività: la prima, necessaria ai fini del completamento dell'ispezione annuale sugli archivi EUROPOL, consiste in accertamenti/verifiche puntuali sulla base delle specifiche segnalazioni inviate dal team ispettivo, tramite il segretariato dell'ACC, ad una o più autorità di protezione dati; la seconda, invece, consiste nell'esercizio del più generale ruolo di controllo delle autorità di protezione dati. Al segretariato è stato assegnato il compito di predisporre una bozza di modulo uniforme per le risposte da fornire al termine delle attività di accertamento/verifica di tipo puntuale.

L'Autorità di controllo comune, ricostituita a seguito dell'entrata in vigore della nuova base giuridica, ha tenuto la sua prima riunione il 9 marzo 2010, eleggendo il Presidente (la portoghese Cruz) ed il Vicepresidente (la slovena Pirc).

L'ACC ha approvato il rapporto sull'ultima ispezione annuale, svolta, nel marzo 2010, sugli archivi di lavoro per fini di analisi e sul sistema di informazione EUROPOL, integrato con le risultanze delle attività di verifica specifiche operate, su segnalazione, a livello nazionale.

Si ricorda, inoltre, che l'Autorità di controllo comune è tenuta a fornire un parere nell'ambito della procedura di approvazione da parte del Consiglio dell'Unione europea degli accordi negoziati tra EUROPOL e Paesi terzi. A riguardo l'ACC ha adottato pareri relativi alla conclusione di accordi sullo scambio di dati con la Repubblica di Macedonia e con Israele, con i quali, pur ravvisando l'opportunità di introdurre specifiche garanzie, si è formulato un giudizio globalmente positivo.

Per quanto riguarda la Colombia, dopo un primo parere negativo (del 9 marzo 2010), che ha evidenziato alcuni punti critici sull'adeguatezza dell'accordo in materia di protezione dati (applicazione delle misure di salvaguardia solo ai dati contenuti in banche dati, inquadramento giuridico dell'accordo nell'ambito della gerarchia delle norme dell'ordinamento colombiano, esercizio del diritto d'accesso da parte degli interessati, termini per la conservazione e la cancellazione dei dati), l'Autorità di controllo comune, con parere del 10 maggio 2010 ha espresso parere favorevole alla conclusione dell'accordo tra Colombia ed EUROPOL.

È stato poi adottato un parere favorevole in relazione al progetto di accordo tra EUROPOL ed il Principato di Monaco, ritenendo adeguato il livello di protezione dei dati personali offerto dal Principato nel quadro della cooperazione con EUROPOL.

Un parere fortemente critico è stato formulato, invece, sulla possibilità per EUROPOL di ricevere informazioni provenienti da parti private.

Nei giorni 18 e 19 ottobre 2010 si è tenuta, a L'Aja, la conferenza sulla protezione dei dati personali organizzata da EUROPOL con la Federazione russa. La Conferenza ha consentito di chiarire diversi aspetti relativi alla legislazione ed alla prassi amministrativa della Federazione russa nel campo della protezione dati, inclusi i poteri e l'organizzazione dell'autorità di supervisione sui trattamenti di dati personali (*Raskomnadzor*). Al termine dei lavori sono stati fissati alcuni punti condivisi, che saranno utili ad EUROPOL per negoziare eventuali accordi operativi per lo scambio di dati con la Federazione russa. Gli schemi di

accordo dovranno comunque essere sottoposti al parere dell'Autorità di controllo comune, che, in precedenti pareri, ha già sottolineato le perplessità e i punti critici per quanto riguarda, in modo specifico, il trattamento dei dati personali da parte delle autorità di polizia della Federazione russa.

Quanto ai nuovi compiti affidati ad EUROPOL dall'accordo sul trasferimento di dati relativi alla messaggistica finanziaria (*cd.* "accordo *TFTP2*") tra Stati Uniti e Unione europea, l'ACC ha deciso di svolgere una prima verifica, utilizzando il team di esperti per le ispezioni, per accertare quali dati sono richiesti dal Dipartimento del tesoro tramite EUROPOL ed a quali trattamenti sono sottoposti. In seguito a questa "*fact finding investigation*", potranno essere discussi ed analizzati gli aspetti di congruenza dell'attività svolta da EUROPOL nel contesto dell'accordo *TFTP2* con quanto previsto dalla Decisione EUROPOL.

La relazione sull'ispezione svolta presso EUROPOL è stata approvata nel corso della riunione straordinaria dell'Autorità di controllo comune svoltasi a Lubiana il 31 gennaio 2011 e, subito dopo, è stata messa a disposizione delle autorità di protezione dati partecipanti alla valutazione congiunta dell'accordo *TFTP2* in rappresentanza del Gruppo Art. 29.

Infine, si è tenuto il 1° febbraio 2011, sempre a Lubiana, l'incontro delle autorità di controllo comune EUROPOL, EUROJUST, Schengen e Dogane per valutare e discutere, tra l'altro, eventuali specifici contributi da offrire in relazione alla Comunicazione della Commissione del 4 novembre 2010 "*Un approccio globale alla protezione dei dati personali nell'Unione europea*", per quanto concerne, in particolare, gli aspetti di integrazione dell'area *cd.* "terzo pilastro" e le conseguenti modifiche delle forme di supervisione congiunta.

Altri punti di interesse in discussione hanno riguardato: la definizione delle strategie delle autorità di controllo comune in relazione alle forme di comunicazione da adottare per informare i cittadini sui compiti e sull'attività svolta, l'applicazione del principio di disponibilità, le modalità di connessione di EUROPOL al SIS.

Si segnala che è stato attivato, nel corso del 2010, il nuovo sito *web* dell'Autorità di controllo comune EUROPOL (*http://europoljsb.consilium.europa.eu*), nel quale sono disponibili, anche in italiano, i principali documenti adottati, nonché informazioni agli interessati su come esercitare i diritti di accesso e gli altri diritti connessi.

Altro aspetto di grande importanza attiene all'attività del comitato per i ricorsi dell'ACC. Si ricorda brevemente che un richiedente può esercitare il diritto di accesso alle informazioni che lo riguardano in possesso dell'EUROPOL, nonché ottenere che tali informazioni siano verificate, corrette o cancellate. Qualora ritenga che l'EUROPOL non abbia fornito una risposta soddisfacente, il richiedente può ricorrere avverso la decisione al comitato per i ricorsi, le cui decisioni sono definitive per tutte le parti coinvolte.

Al riguardo, si segnala che il Comitato ha ricevuto ed esaminato, in quanto ritenuti ammissibili, 3 ricorsi, sui quali una formale decisione è stata assunta nel corso della riunione di dicembre 2010.

Il Sistema informativo doganale (SID): *CIS - Supervision Coordination Group* e Autorità comune di controllo

L'8 marzo 2010 si è tenuta la prima riunione, convocata dall'EDPS, della nuova autorità di supervisione (*CIS - Supervision Coordination Group*) sul sistema informativo Dogane. Nell'incontro, i rappresentanti della Commissione europea e dell'OLAF hanno illustrato la nuova base giuridica per l'utilizzo del SID: il Regolamento (CE) n. 515/97 del 13 marzo 1997 (cfr., in particolare, art. 37), relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione della normativa doganale e agricola, nonché, nell'ambito della cooperazione giudiziaria e di polizia, la Decisione 2009/917/GAI del 30 novembre 2009, la cui entrata in vigore è prevista per il 27 maggio 2011.

In considerazione della sopravvenuta coesistenza di due forme di supervisione per un'unica banca dati (il SID - Sistema informativo doganale), si è ritenuto di definire modalità di cooperazione il più possibile integrate per evitare riunioni in tempi diversi dei due organismi di supervisione (ACC Dogane e *CIS - Supervision Coordination Group*).

Per quanto riguarda l'attività di verifica e controllo dei trattamenti dei dati nell'ambito del SID, è stato elaborato un questionario da completare a cura delle autorità competenti degli Stati membri (per l'Italia, Agenzia delle Dogane) per l'autovalutazione degli aspetti relativi all'idoneità delle misure di sicurezza adottate ed alla formazione del personale su tali misure.

Il questionario di *self assessment* è stato inviato, con osservazioni anche sulla possibile revisione della struttura e dei quesiti, dal Garante al Segretariato della ACC, che esaminerà

e confronterà le risposte fornite dalle autorità competenti dei diversi Stati aderenti al sistema informativo doganale.

Riguardo l'organizzazione dell'ispezione al SID centrale (C.CIS) a Bruxelles, è previsto un gruppo ispettivo composto da un rappresentante del segretariato dell'Autorità di controllo comune e da altri tre rappresentanti.

Il Sistema informativo Schengen: valutazione Schengen dell'Italia e attività dell'ACC

Il 27 gennaio 2010 si è svolta la valutazione Schengen dell'Italia per gli aspetti relativi alla protezione dei dati personali riferiti alla sezione nazionale del Sistema informativo Schengen (N.SIS).

Nel corso della visita presso il Garante sono state illustrate l'organizzazione e la struttura dell'autorità, i poteri e le competenze, nonché le modalità di esercizio del ruolo di supervisione e controllo sui trattamenti di dati personali nel settore polizia e giustizia. Inoltre, sono stati trattati i temi dell'esercizio dei diritti di accesso, rettifica e cancellazione da parte degli interessati e della cooperazione con le altre autorità di protezione dei dati dei Paesi Schengen con specifico riferimento a richieste riguardanti segnalazioni inserite nel sistema informativo da altri Paesi.

Il gruppo di esperti ha altresì approfondito, presso la sede di N.SIS e Divisione SIRENE del Ministero dell'interno, l'esame dell'organizzazione di tali servizi e delle modalità di esercizio del diritto di accesso.

All'esito di tale procedura, il Gruppo di esperti ha espresso una valutazione nel complesso positiva ed ha formulato alcune raccomandazioni, in linea con le prescrizioni emanate dal Garante, volte a intensificare le misure di sicurezza poste a tutela di dati e sistemi.

Inoltre, si segnala che il 3 maggio 2010 si è tenuta, presso il Consiglio dell'Unione europea, la riunione del "*Working Party on Schengen Evaluation*", relativa, tra l'altro, alla presentazione del rapporto (formalmente adottato nella riunione di giugno) redatto dal gruppo di esperti a conclusione della visita svolta in Italia a gennaio. Il rapporto contiene, in particolare, specifiche raccomandazioni, rivolte sia al Garante sia al Ministero dell'interno. Il citato *Working Party* ha contestualmente dato l'avvio al monitoraggio dell'attuazione, da parte del Ministero dell'interno, delle raccomandazioni previste dal rapporto.

A margine, è in corso l'attività di revisione delle modalità con le quali si procede alle

valutazioni Schengen per i singoli Paesi. A tal fine, la Commissione europea ha presentato il 19 novembre 2010 una proposta di regolamento per il successivo esame da parte del Consiglio dell'Unione europea. Il Ministero dell'interno ha svolto una prima riunione di coordinamento per analizzare i primi nove articoli del testo il 15 dicembre 2010.

Per quanto riguarda la composizione dell'ACC, nel mese di marzo l'Autorità comune di controllo Schengen ha rinnovato i vertici eleggendo, come presidente, la tedesca Angelika Schriever-Steinberg e come vicepresidente, lo svizzero Jean Philippe Walter.

In relazione all'attività di controllo sul Sistema d'informazione Schengen, l'ACC ha programmato il nuovo calendario di verifiche da svolgere con riguardo alle segnalazioni inserite nel SIS. A tal fine, il Segretariato ha predisposto una *checklist* per le verifiche, basata sulle raccomandazioni formulate dalla stessa autorità comune di controllo. Per l'anno 2011, l'ACC si propone, in modo specifico, di effettuare attività di verifica sugli inserimenti nel SIS di segnalazioni su richiesta delle autorità giudiziarie.

Inoltre, le delegazioni sono state invitate a fornire elementi sul seguito dato alle raccomandazioni formulate dall'ACC al termine dell'azione comune sulla verifica della correttezza dell'inserimento nel SIS di segnalazioni *ex* art. 96 della Convenzione (stranieri segnalati ai fini della non ammissione). Sulla base degli elementi ricevuti l'ACC ha adottato il *report* ("*Report of the Schengen Joint Supervisory Authority on the follow-up of the recommendations concerning the use of Article 96 alerts in the Schengen Information System*").

L'Autorità di controllo comune ha inoltre deciso di completare le verifiche con riferimento alle segnalazioni inserite nel SIS *ex* art. 95 della Convenzione (persone ricercate per arresto a fini di estradizione). A tal fine, il Segretariato sta predisponendo il modello di questionario da sottoporre alle competenti autorità nazionali.

Sono invece ancora in corso di definizione le modalità e la tempistica per la valutazione del *follow-up* dell'attività di controllo delle segnalazioni inserite nel SIS in base all'art. 99 della Convenzione (dati relativi a persone o veicoli inseriti a fini di sorveglianza discreta o controllo specifico).

È stata poi valutata l'opportunità di svolgere una nuova campagna informativa sui diritti degli interessati in relazione ai Sistemi informativi Schengen. Si ricorda che l'Autorità di

controllo comune Schengen dovrebbe terminare i suoi lavori con l'entrata in vigore del nuovo sistema SIS II (presumibilmente operativo dal 2013), al quale si applicherà (in senso analogo a quanto previsto per EURODAC) un modello di supervisione centrato sul ruolo del Garante europeo dei dati personali. Al riguardo si anticipa, che in tale sistema sarà possibile integrare nuove funzioni e dati (ad es., *link* tra segnalazioni, inserimento di impronte digitali) e che la gestione del sistema potrebbe essere affidata ad un'autorità appositamente costituita per garantire la funzionalità dei *cd.* "grandi sistemi informativi europei" ("*large scale database*": SIS, VIS, EURODAC).

È stato inoltre deciso di procedere all'ispezione presso l'unità di supporto tecnico (C.SIS) a Strasburgo, ed a tal fine è stata richiesta assistenza tecnica alle delegazioni.

Si è poi discusso il tema dell'accesso di EUROPOL al SIS ed è stato adottato il rapporto contenente il *follow-up* delle azioni svolte a livello nazionale per dar seguito alle raccomandazioni formulate nel rapporto del 2006.

EURODAC (Eurodac Supervision Coordination Group): attività dell'ACC

L'*EURODAC Supervision Coordination Group* si è riunito l'8 Marzo 2010 sotto la presidenza dell'EDPS. La svedese Wallin è stata eletta vicepresidente.

Sono stati discussi i documenti relativi al programma di attività della Autorità di controllo comune per il biennio 2008-2009 ed il programma di lavoro 2010-2011. È stato inoltre distribuito alle delegazioni il testo finale delle raccomandazioni sull'uso di DubliNet, la rete di comunicazione utilizzata dalle amministrazioni nazionali competenti ai fini dell'individuazione dello Stato competente per l'esame della domanda di asilo.

L'ACC, che ha anche trattato il tema del possibile accesso ad EURODAC da parte delle forze di polizia, ha invitato ad una riunione le organizzazioni internazionali maggiormente attive nel settore dell'asilo (ACNUR, ECRE) per informazioni sull'attività svolta e ai fini di una migliore comprensione dei problemi di più pressante attualità.

20.4. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Case Handling Workshop

I due incontri annuali per l'anno 2010 dedicati al *Case Handling* si sono tenuti rispettivamente il 18-19 marzo a Bruxelles ed il 20-21 settembre a Manchester.

Durante l'incontro di Bruxelles, e sulla base delle indicazioni fornite dalla *Spring*

Conference 2009, il gruppo ha proseguito in parte i lavori avviati in occasione dell'incontro di Cipro nell'autunno 2009. In particolare, è stato nuovamente affrontato il tema dell'esercizio del diritto di accesso con riferimento alle problematiche sollevate dall'interpretazione dell'art. 12, par. 1, lett. *a*), della direttiva, contenuta nella sentenza della Corte di Giustizia del 7 maggio 2009 (caso *College Van Burgemeester en Wethouders Van Rotterdam vs M. E. E. Rijkeboer*), che fa riferimento al diritto per l'interessato di ottenere informazioni su "destinatari o categorie di destinatari cui sono comunicati i dati". Inoltre, i Paesi Bassi hanno presentato, nell'ambito della medesima sessione, un progetto di legge governativo *cd.* "*pay as you drive*", che dovrebbe consentire il pagamento delle tasse automobilistiche in base all'utilizzo delle vetture (a seconda dei chilometri percorsi, degli orari in cui la vettura è utilizzata, ecc.) e di cui è valutato l'impatto con la *privacy*.

Si rileva, inoltre, che nel corso della sessione dedicata agli "*hot topics*" è stato affrontato il tema del "*behavioural advertising*", oggetto di un apposito parere del Gruppo Art. 29, e sono state analizzate le possibili conseguenze derivanti dalle modifiche apportate alla Direttiva n. 2002/58/CE, in particolare l'utilizzo dei "*cookies*". Al riguardo, si è osservato che l'attuale sistema di "*opt out*" previsto dall'art. 5.3 della direttiva dovrà essere sostituito da un approccio orientato al consenso preventivo ("*opt in*"). Si è anche discusso del tema dei trattamenti effettuati con *Google Street View*, riportando le relative esperienze nazionali, mentre l'autorità federale tedesca di protezione dati ha illustrato la recente sentenza della Corte Costituzionale tedesca che ha dichiarato l'incostituzionalità della normativa nazionale di recepimento della Direttiva n. 2006/24/CE.

L'incontro di Manchester presso l'*Information Commissioner* del Regno Unito, in occasione del decennale dell'istituzione dei seminari in parola, ha avuto per oggetto l'approccio complessivo delle autorità europee di protezione dati nella trattazione della casistica, con riferimento a quattro fasi ritenute sostanzialmente di comune esperienza: il primo contatto con l'Autorità, l'esame delle eventuali segnalazioni o dei ricorsi presentati, le attività di *audit* (controllo preventivo) e le attività di *enforcement* (controllo *ex-post*). Il dibattito ha consentito di evidenziare le numerose differenze tra le procedure adottate, in ragione delle diverse tradizioni giuridiche e culturali e dei diversi poteri conferiti alle autorità dal diritto

nazionale (ad es., non tutte le autorità sono in grado di imporre sanzioni o di svolgere ispezioni). Si è comunque concordato sull'opportunità di una certa flessibilità nella gestione dei casi attraverso uno *screening* che, allo stato, solo poche autorità europee possono svolgere. Tale valutazione preventiva potrebbe consentire alle autorità di concentrare lo sforzo e le risorse su tematiche che presentino un impatto maggiore in termini di lesione del diritto fondamentale alla protezione dei dati.

IWGDPT: il "Gruppo di Berlino" - *International Working Group on Data Protection in Telecommunication*

L'Autorità ha partecipato ai due consueti incontri semestrali dell'*International Working Group on Data Protection in Telecommunication* (*IWGDPT*) il 15-16 aprile 2010 a Granada e il 6 e 7 settembre 2010 a Berlino. Nel corso della prima riunione è stata approvata la Granada *Charter of Privacy* in *a Digital World* che, muovendo dal presupposto che nel nuovo mondo interattivo gli individui più che semplici utenti sono cittadini portatori di diritti inalienabili, raccomanda ai fornitori di servizi di comunicazione, alle autorità pubbliche e agli stessi individui che si servono di tali servizi, di osservare le garanzie a tutela degli interessati affinché la libera circolazione delle informazioni avvenga nel rispetto della dignità, della *privacy* e della protezione dei dati. In particolare la Carta di Granada sottolinea la necessità di fornire agli utenti informative complete sul tipo di trattamento dei dati e sul livello della loro diffusione, nonché l'opportunità che le Autorità di protezione dei dati si rendano promotrici di campagne informative, soprattutto rivolte alle nuove generazioni, sull'uso consapevole e responsabile dei servizi di comunicazione elettronica. Nello stesso incontro è stata affrontata la questione della possibile riattribuzione, ad un nuovo utente, di indirizzi di posta elettronica precedentemente utilizzati e dismessi da un altro titolare dell'*account*. La discussione ha portato all'integrazione del documento approvato durante l'incontro del 7-8 settembre 2009 a Berlino, che fornisce raccomandazioni ai fornitori di servizi di comunicazione elettronica ed agli stessi utenti per evitare che si verifichino violazioni della *privacy* e della sicurezza dei dati a seguito della riallocazione di indirizzi di posta elettronica e di servizi analoghi della *cd.* "*società dell'informazione*" (v. *Relazione* 2009, p. 285 ss.).

Nella riunione di Berlino è stata esaminata, fra l'altro, la questione della "*deep packet inspection*" (*DPI*), tecnica che consente la verifica dei pacchetti-dati in transito su una rete

esaminandone i contenuti, oggi adoperata in misura crescente anche per la gestione del traffico di dati, per il controllo della diffusione di contenuti illegali, compresi quelli in violazione dei diritti d'autore, per l'invio di pubblicità mirata. Il gruppo –nel documento di lavoro approvato durante l'incontro– ha espresso forti riserve sull'applicazione della *DPI* per scopi diversi dal mantenimento della sicurezza del sistema informatico e delle reti o dalle legittime finalità previste dalla legge. In particolare, è stato rilevato che l'impiego di simili tecniche può comportare l'indebita violazione della segretezza delle comunicazioni ed è stato raccomandato ai fornitori di accesso a Internet di astenersi dall'uso della *DPI* a fini di pubblicità comportamentale.

Nello stesso incontro è stato anche affrontato il tema della sicurezza dei dati con riferimento ai dispositivi mobili quali telefonini, *smart phone* e *laptop* che, per le caratteristiche tecniche e d'uso, sono esposti in special modo alla manipolazione, alla perdita e al furto di dati. In proposito, il gruppo ha fornito le prime raccomandazioni, rivolgendosi sia ai fornitori, affinché assicurino il massimo livello di sicurezza in relazione alla finalità del dispositivo e informino in maniera chiara e adeguata gli utenti sulle impostazioni di sicurezza, sia agli utenti stessi, i quali possono contribuire ad evitare o ridurre i rischi per l'integrità, la confidenzialità e la sicurezza dei dati.

L'incontro di Berlino ha rappresentato anche l'occasione per lo scambio di informazioni tra le diverse Autorità riguardo a problematiche di stringente attualità, quali: *Google Street View*, l'utilizzo dei *social network*, la profilazione dei clienti da parte degli operatori delle telecomunicazioni, le misure di sicurezza adottate dai fornitori di servizi Internet, le banche dati nel settore delle telecomunicazioni, la portabilità del numero telefonico, le regole tecniche per l'utilizzo delle tecnologie dell'informazione/comunicazione nei procedimenti giudiziari di natura civile e penale.

Con riferimento ai *social network*, anche a seguito della presentazione da parte dell'Autorità canadese dei risultati di attività ispettive in particolare con riferimento all'uso di dati per scopi commerciali da parte di soggetti terzi, è emersa la necessità: di fornire un'informativa dettagliata sui dati impiegati e sulle finalità commerciali del trattamento (e non già un'indicazione generica su una possibile comunicazione di dati a soggetti terzi);

di valorizzare i princìpi già espressi nel *Memorandum* di Roma, adottato in occasione del 43mo incontro del Gruppo tenutosi a Roma il 3-4 marzo 2008 (v. *Relazione* 2008, p. 232); di introdurre strumenti di controllo sui contenuti aperti anche ai non utenti.

A Berlino è inoltre proseguita la riflessione sul tema dei dispositivi, posti su autoveicoli, in grado di registrare eventi particolari quali incidenti e malfunzionamenti. Tale problematica sarà oggetto di un apposito documento di lavoro, mentre è stata avviata la discussione sul tema della geolocalizzazione attraverso dispositivi mobili, già ampiamente utilizzati in alcuni Stati membri. Ci si riferisce in particolare al *cd.* "*foursquare*", un *social network* per la geolocalizzazione che sfrutta le funzionalità *GPS* degli *smartphone*: uno strumento dalle potenzialità enormi –sia per gli utenti sia per le aziende e le attività commerciali alla ricerca di spazi pubblicitari– che desta perplessità soprattutto in relazione alla proporzionalità del trattamento dei dati personali.

Consiglio d'Europa

Nel corso del 2010 l'Autorità ha proseguito la sua partecipazione ai lavori del Comitato consultivo (T-Pd) della Convenzione 108/1981 del Consiglio d'Europa, contribuendo anche alle attività del T-Pd Bureau, il gruppo ristretto volto ad assicurare continuità ai lavori del T-Pd.

Il Comitato consultivo ha concluso i lavori per la Raccomandazione in materia di profilazione, adottata dal Comitato dei ministri il 23 novembre 2010.

La Raccomandazione, pur riconoscendo agli Stati la facoltà di non applicare alcuni princìpi ove necessario per la sicurezza nazionale, la pubblica sicurezza, gli interessi monetari del Paese, la prevenzione e persecuzione dei reati o per proteggere l'interessato o i diritti e le libertà di terzi, detta le condizioni della profilazione in ambito pubblico e privato. Il testo mira a fornire agli interessati un quadro di garanzie idoneo, considerato che la profilazione consente la raccolta massiccia di dati e la loro aggregazione automatica secondo classi di appartenenza. In particolare la Raccomandazione garantisce il diritto dell'interessato ad una scelta informata e consapevole, attraverso la previsione dell'obbligo di informativa, della richiesta del consenso ove necessario, del rispetto dei princìpi di proporzionalità, necessità e finalità. All'interessato è riconosciuto un ampio diritto di accesso, con particolare riferimento alla logica del trattamento, nonché il diritto di opporsi a

decisioni che abbiano ripercussioni sulla sua persona, basate sulla sola profilazione. Per i titolari è previsto l'obbligo specifico di garantire la sicurezza dei dati, nonché di assicurare la correttezza degli stessi limitando i rischi di errore inerenti a tale tecnica di trattamento.

Al termine del lavoro in materia di profilazione, le attività del T-Pd si sono concentrate sul processo di revisione della Convenzione 108/1981. Come avvenuto per l'OCSE e per l'Unione europea, anche nell'ambito del Consiglio d'Europa si è avvertita l'esigenza di verificare se, a trent'anni dalla loro approvazione, i princìpi della Convenzione siano ancora in grado di fornire un'adeguata tutela per i diritti delle persone.

Il T-Pd ha dato pertanto inizio al lavoro di approfondimento attraverso l'esame del Rapporto –prodotto dagli esperti del *Centre de Recherches Informatique et Droit* (*CRID*) di Namur– sulle possibile lacune della Convenzione a fronte del più recente sviluppo tecnologico. Lo studio rappresenta una prima riflessione sugli aspetti più problematici che derivano dall'applicazione dei princìpi della Convenzione 108/1981 nel mutato scenario tecnologico, funzionale ad una possibile revisione della stessa Convenzione. In particolare, nel documento è stata valutata: la possibilità di prevedere modifiche in merito allo scopo, all'ambito di applicazione della Convenzione ed al suo impianto definitorio; l'introduzione di un regime speciale per il trattamento dei dati di traffico e di localizzazione; la maggiore estensione del principio di proporzionalità; l'inserimento del consenso dell'interessato tra i requisiti di legittimità del trattamento; l'introduzione del principio di minimizzazione dei dati; la revisione della nozione di dati sensibili; l'ampliamento degli obblighi di sicurezza dei dati, di trasparenza del trattamento e dell'esercizio dei diritti; l'introduzione del diritto a non essere destinatario di decisioni fondate puramente su trattamenti automatizzati, del diritto "a non essere tracciato" e del diritto ad una navigazione sul *web* anonimizzata; l'introduzione dei princìpi di *accountability*, *privacy by design* e *privacy impact assessment*; la previsione di un regime speciale per il trattamento dei dati che riguardano i minori.

Nell'ambito della riflessione sulla tenuta dei princìpi di protezione dati alla luce delle nuove tecnologie e del processo di globalizzazione, il T-Pd ha anche avviato un lavoro sulla possibile revisione delle Raccomandazioni del Consiglio d'Europa; in particolare,

sulla base dello studio del prof. Joseph A. Cannataci della *University of Central Lancashire*, Preston, sulle criticità, rispetto al contesto attuale, della Raccomandazione (87)15 relativa al trattamento dei dati personali nell'ambito di polizia. Alla luce del Rapporto presentato dal dott. Giovanni Buttarelli –Garante europeo aggiunto per la protezione dei dati– è stata invece avviata la discussione sulla Raccomandazione (89)2 in materia di trattamento dei dati in ambito lavorativo a fronte delle innovazioni tecnologiche degli ultimi anni, con specifico riferimento ai temi del controllo del lavoratore, della dimensione globale del settore, della diffusione dell'*outsourcing* su scala internazionale, delle esigenze, spesso in conflitto con la tutela della *privacy* dei lavoratori, di trasparenza e di pubblicità di dati.

Sempre nell'ambito del Consiglio d'Europa, nel corso della Conferenza dei Ministri di Giustizia di Istanbul del 24-26 novembre 2010 sono state approvate due risoluzioni. La prima, "*Data protection* e *privacy* nel terzo millennio", sostiene l'opportunità di modernizzare la Convenzione 108/1981 affinché possa continuare ad offrire un'adeguata tutela alla luce delle nuove tecnologie, incoraggia gli Stati a ratificare la stessa Convenzione e invita il segretario generale a considerare la protezione dei dati come prioritaria nell'ambito del Consiglio d'Europa. La seconda, su "una giustizia moderna, trasparente ed efficiente", prevede una revisione delle diverse raccomandazioni del Consiglio che riguardano l'applicazione delle nuove tecnologie in materia di giustizia, invita i Comitati competenti ad avviare un lavoro per la predisposizione di *standard* nell'uso delle nuove tecnologie nel settore della giustizia e istituisce un Osservatorio europeo permanente sui tempi della giustizia.

Nel corso dell'anno è stata confermato nella carica di *Data Protection Commissioner* del Consiglio d'Europa il commissario Neuwirt.

Infine, nell'ambito della consueta attività di coordinamento riguardo al "*Data protection day*", anche l'anno in esame è stato caratterizzato da un intenso lavoro del Consiglio d'Europa volto a rendere pubbliche le diverse iniziative intraprese in materia dalle varie autorità nazionali interessate. In occasione della Giornata per la protezione dei dati, il Consiglio d'Europa ha lanciato –attraverso il sito *web* istituzionale– la consultazione pubblica relativa al processo di revisione della Convenzione 108/1981.

OCSE - *WPISP*

In ambito OCSE, il *Working Party on Information Security and Privacy* (*WPISP*) ha proseguito i suoi lavori nel corso del 2010, in modo particolare sulla revisione delle linee-guida sulla protezione della *privacy* (che risalgono al 1980) e i flussi transfrontalieri di dati, alla luce delle nuove sfide che la protezione dei dati è chiamata ad affrontare. L'OCSE, in occasione del 30° anniversario delle linee-guida, ha organizzato tre eventi: *la Roundtable on the Impact of the Privacy Guidelines* (Parigi, 10 marzo 2010); *la Conference on the Evolving Role of the Individual in Privacy Protection* (Gerusalemme, 25-26 ottobre 2010, a margine della Conferenza internazionale delle Autorità per la protezione dei dati); *la Roundtable on the Economic Dimensions of Personal Data and Privacy* (Parigi, 1 dicembre 2010). Nel corso dei suddetti eventi è stato messo in luce il ruolo che l'individuo oggi svolge con riferimento alla protezione dei dati, specie in considerazione delle nuove tecnologie interattive, nonché il crescente valore economico che *privacy* e protezione dei dati hanno assunto nel corso degli anni. Nel corso dei tre eventi è stato, inoltre, concordato dai partecipanti che il nuovo testo delle linee-guida dovrà essere redatto nella maniera più flessibile possibile, utilizzando un linguaggio semplice, con l'auspicio che possa essere condiviso dalle ventuno economie dei più grandi Paesi del mondo.

Parallelamente, l'OCSE ha avviato l'elaborazione del Rapporto "*The Evolving Privacy Landscape*", che dovrebbe essere reso pubblico nel corso del 2011 e nel quale vengono identificati i punti di forza e le criticità delle linee-guida anche in vista della possibile revisione. Il processo di revisione sarà avviato con il coinvolgimento delle diverse delegazioni che partecipano all'OCSE, compresi i rappresentanti del mondo dell'industria e della società civile, che saranno chiamati a fornire il proprio punto di vista attraverso un apposito questionario.

Il lavoro del *WPISP* in ambito OCSE si è poi concentrato sulla *Privacy Enforcement Cooperation* e sulla necessità ulteriore di cooperazione tra le Autorità, specie tramite la designazione di appositi punti di contatto nazionali, lo scambio di informazioni e la stipula di accordi globali o bilaterali tra diverse autorità. Ha approfondito altresì il *cd.* "*identity management*", con particolare riferimento alle diverse strategie poste in essere dai diversi Paesi, nonché la *e-authentication*, svolgendo un'analisi della persistente attualità ed

efficacia della Raccomandazione OCSE del 2007. Ha infine esaminato la protezione dei minori *online*, con la presentazione di un rapporto sui rischi e i pericoli ai quali sono esposti i minori.

Il Gruppo ha inoltre riservato uno spazio particolare al tema della sicurezza in rete (*cybersecurity*, *software security*, lotta al *malware*) e ha dato inizio ad un lavoro rivolto all'analisi comparata delle strategie nazionali di *cybersecurity*, con particolare riferimento all'iniziativa sulla sicurezza in Internet promossa dall'Autorità australiana per le comunicazioni e i media (ACMA) per incoraggiare gli Internet *service provider* a contattare i clienti per fornire una guida per il ripristino della sicurezza dei propri *computer*, laddove compromessa. Il Gruppo ha mostrato grande interesse per il progetto, approvando la proposta australiana di intraprendere un simile lavoro nell'ambito del *WPISP*. Tale progetto potrebbe eventualmente essere inglobato in un'iniziativa internazionale per contrastare le attuali e future minacce alla *cybersecurity* degli utenti.

Incontri con delegazioni estere

Nel 2010 è proseguita l'attività di cooperazione con le autorità per la protezione dei dati di altri Paesi. Oltre agli incontri con i funzionari esperti dei Ministeri dell'Interno della Romania (febbraio 2010) e della Turchia (marzo 2010) (v. *Relazione* 2009, p. 288), l'Autorità, nell'ambito del programma *TAIEX* della Commissione europea, ha ospitato nel mese di aprile alcuni rappresentanti dell'autorità di protezione dati della Repubblica moldava, anche in vista di un eventuale accesso della Moldavia all'Unione europea. Nel mese di gennaio 2011, nell'ambito di un Progetto di gemellaggio (*Twinning*) finanziato dalla Comunità europea per aiutare Israele a completare la fase di avvio dell'Autorità di protezione dei dati, si è svolta presso il Garante una visita di studio di alcuni rappresentanti dell'autorità israeliana.

L'incontro, che è stato focalizzato principalmente sul tema dell'*inforcement*, ha incluso anche una visita presso il Nucleo speciale *privacy* della Guardia di finanza.

21. Le attività di comunicazione, studio e ricerca

21.1. La comunicazione del Garante: profili generali

Le nuove regole per la videosorveglianza, i servizi offerti da *Google Street View*, l'uso disinvolto dei *social network*, il nuovo regime del *telemarketing*, l'attività di profilazione degli utenti da parte di aziende e fornitori di servizi di comunicazione elettronica, alle regole per la diffusione *online* dei documenti della p.a., il corretto rapporto tra diritto di cronaca e tutela dei minori, il bilanciamento tra trasparenza e riservatezza. Sono questi i temi su cui maggiormente si è focalizzata l'attività di informazione svolta nel 2010, a dimostrazione della volontà del Garante di affrontare, quando non di anticipare, i complessi problemi che la società contemporanea ci pone davanti, con l'obiettivo di far crescere la consapevolezza del valore da attribuire ai dati personali e della necessità di una loro adeguata protezione e messa in sicurezza.

Privilegiando un linguaggio chiaro e divulgativo, anche attraverso indicazioni operative per l'attuazione corretta delle norme, grande impegno è stato posto nel dare conto puntualmente degli interventi sui quali si è concentrato il lavoro dell'Autorità, con particolare riguardo ai settori di maggiore interesse sociale. Tra questi, vanno ricordati i nuovi servizi offerti in Internet, come la localizzazione, o i nuovi sistemi di gestione dati *online* come il *cloud computing*; i nuovi sistemi di controllo agli aeroporti, come i *body scanner*; le intercettazioni; le comunicazioni private captate sulle reti *Wi Fi*; lo *spam* via fax e via e-mail; la ricerca medica e la sanità; il mondo della scuola; la tutela dei disabili; le grandi banche dati sia pubbliche che private che richiedono l'adozione di nuove misure di sicurezza per evitare intrusioni illecite o furti di dati personali; le centrali rischi; il rispetto della dignità delle persone malate; la regolamentazione della propaganda elettorale; la tutela dei lavoratori.

La presenza sui *media* delle tematiche riguardanti la protezione dei dati personali ed in particolare l'attività del Garante, ha confermato un *trend* in crescita.

Nel periodo dal 1° gennaio al 31 dicembre 2010 il Servizio relazioni con i mezzi di informazione ha selezionato oltre 24.700 articoli di interesse dell'Autorità. Sulla base della

rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media online*, che hanno dedicato spazio alle questioni legate generalmente alla *privacy*, sono state circa 13.000, delle quali 3.300 dedicate esclusivamente all'attività del Garante. Le prime pagine riguardanti i temi della protezione dei dati personali sono state oltre 800 (di cui 170 riguardanti la sola Autorità). Numerose sono state le interviste, gli interventi e le dichiarazioni pubblicate sulla carta stampata (214) e andate in onda su tv e radio nazionali e locali (100). Le citazioni relative all'attività del Garante in programmi televisivi e radiofonici nazionali sono state oltre 300.

21.2. I PRODOTTI INFORMATIVI

Nel corso del 2010 l'Autorità ha diramato 27 comunicati stampa e 12 *Newsletter*.

La *Newsletter*, giunta al suo XII anno di pubblicazione (per un totale di 344 numeri e di 1.195 notizie) nella versione *online* è stata rinnovata completamente, sia nella grafica che nella nuova disposizione dei testi. Da tempo stabile strumento di riferimento dell'attività di comunicazione del Garante, la *Newsletter* privilegia un'approfondita informazione sui provvedimenti adottati e sull'attività nazionale ed internazionale dell'Autorità. La consultazione *online* e l'invio telematico ad un numero sempre crescente di abbonati (istituzioni, pp.aa., imprese, liberi professionisti, giornalisti, privati cittadini) hanno notevolmente ampliato la diffusione e favorito l'apprezzamento da parte di un vasto pubblico.

Il *Dvd* "*Il Garante e la protezione dei dati personali*", giunto alla XX edizione, contiene un archivio multimediale aggiornato che consente di consultare *full text* la normativa nazionale e internazionale, i provvedimenti adottati dall'Autorità, la raccolta completa dei comunicati stampa e delle *Newsletter*. Il *Dvd* viene inviato a quanti ne fanno richiesta e distribuito al largo pubblico in occasione di manifestazioni nazionali, convegni, incontri, seminari che vedono la presenza e la partecipazione del Garante.

Il costante impegno per una comunicazione istituzionale diretta soprattutto verso il cittadino si è concretizzato nella realizzazione di opuscoli divulgativi in grado di illustrare i diversi temi connessi alla protezione dei dati personali. Al recente *vademecum* dedicato ad un uso consapevole dei *social network* ("*Social network: attenzione agli effetti collaterali*"),

nel 2010 si è aggiunto quello dedicato alla protezione dei dati e al rispetto delle persone nell'ambito scolastico dal titolo "*La privacy tra i banchi di scuola*". La guida rivolta a presidi, insegnanti, operatori scolastici, così come a genitori e studenti, ha riscosso significativo successo ed è stata distribuita presso istituti di ogni ordine e grado. Il progetto di comunicazione istituzionale proseguirà con la realizzazione di una ulteriore serie di *dépliant* relativi a diverse tematiche (sanità, condominio, lavoro, videosorveglianza).

21.3. GLI INCONTRI INTERNAZIONALI

Nel corso del 2010 importanti incontri internazionali hanno registrato la presenza dell'Autorità italiana, come indicato, con maggiori dettagli, nella sezione relativa alle Relazioni internazionali.

Dal 27 al 28 ottobre, si è svolta a Gerusalemme la 32ma *Conferenza internazionale dei Garanti*. All'importante manifestazione mondiale hanno partecipato il presidente Pizzetti, il vicepresidente Chiaravalloti e il componente dell'Autorità Giuseppe Fortunato. Al centro dei lavori i temi legati ai nuovi sistemi di comunicazione, alla nuova realtà della Rete, ma anche all'efficacia degli strumenti normativi finora utilizzati. Il presidente dell'Autorità italiana ha presieduto una sessione dedicata allo strumento del consenso all'uso dei dati, uno dei pilastri fondamentali delle normative in materia di protezione dati che rischia oggi –nell'era dei motori di ricerca, dei *social network*, degli *smart phone* e della "profilazione" *online* delle persone– di perdere la sua reale efficacia. "*Internet –ha affermato Pizzetti– ha messo in discussione gli strumenti di tutela messi a punto dalla normativa sulla protezione dei dati e la sfida principale che oggi ci troviamo davanti è quella di pensare nuove regole che aiutino noi, ma soprattutto le nuove generazioni, ad affrontare le nuove realtà*".

La Conferenza internazionale di Gerusalemme delle autorità di protezione dati si è chiusa con l'approvazione, in particolare, di due importanti risoluzioni che significativamente guardano alle soluzioni tecnologiche ed agli approcci transnazionali.

La prima riguarda l'approccio di "*privacy by design*", ossia la necessità di incorporare i princìpi a tutela della *privacy* nella progettazione e nella gestione di qualsiasi sistema o dispositivo telematico o informatico. L'altra risoluzione riguarda la convocazione di una

conferenza intergovernativa che sancisca il valore giuridicamente vincolante dei "*Princìpi internazionali in materia di privacy e protezione dei dati personali*" approvati dalla Conferenza internazionale di Madrid del 2009. La Conferenza ha ammesso nuovi membri fra quelli accreditati: in particolare, la *Federal Trade Commission* degli USA e l'Autorità messicana per la protezione dei dati, che ospiterà la Conferenza del 2011.

Il 9 febbraio, a Roma, è stata celebrata la Giornata della sicurezza in rete (*Safer Internet Day*), che ha avuto tra gli altri anche il patrocinio del Garante. La giornata –istituita nel 2004 nell'ambito del programma *Safer Internet* dalla Commissione europea dedicata alla promozione di un utilizzo sicuro e responsabile delle nuove tecnologie da parte degli utenti più giovani– è giunta alla settima edizione e negli ultimi anni ha superato i confini europei diventando un appuntamento di riferimento a livello internazionale. Tema specifico dell'edizione 2010 è stato quello relativo alla "*Gestione dei dati e delle immagini personali online*". L'obiettivo, quello di stimolare una riflessione sulla gestione della propria e altrui *privacy* in Rete –in particolare per i minori– e sulle possibili conseguenze. Nel corso della manifestazione è stato distribuito il *vademecum* "*Social Network: attenzione agli effetti collaterali*", curato dal Servizio relazioni con i mezzi di informazione e realizzato proprio allo scopo di sensibilizzare le nuove generazioni sui rischi connessi ad un uso non corretto delle nuove tecnologie. In una società virtuale quale quella in cui viviamo, le nuove tecnologie hanno lanciato sfide rilevanti rispetto alla protezione dei dati personali. La "generazione digitale" semina frammenti di informazioni personali che rimarranno per sempre su Internet accessibili a questa e alle future generazioni attraverso una semplice ricerca in rete.

La tradizionale "*Conferenza di primavera delle autorità europee per la protezione dei dati personali*" (*Spring Conference*) del 2010 si è tenuta a Praga dal 29 al 30 aprile 2010. Alla conferenza di primavera, oltre alle Autorità di protezione dei dati degli Stati membri dell'Unione europea e del Consiglio d'Europa, partecipano anche le autorità subnazionali e le autorità di controllo comuni in materia di polizia, giustizia e sicurezza. Il tema principale della conferenza di Praga è stato "*Pensare il passato, pensando al futuro*", proprio con l'obiettivo di discutere sulle nuove sfide per la protezione dei dati e la revisione del quadro legislativo vigente.

Il presidente Pizzetti ha partecipato alla Conferenza con un suo intervento dedicato al tema del rapporto tra trasparenza e riservatezza in relazione alla diffusione di documenti da parte di amministrazioni pubbliche, in particolare sul *web*, dal titolo "*Dati pubblici tra il diritto di sapere e il diritto alla privacy*".

I lavori si sono conclusi con l'adozione di tre importanti risoluzioni: la prima sul previsto accordo tra l'Unione europea e gli Stati Uniti d'America sulle norme di protezione dei dati in materia di polizia e cooperazione giudiziaria in materia penale, la seconda sull'uso dei *body scanner* a fini di sicurezza aeroportuale, la terza sulla messa a punto di azioni congiunte di sensibilizzazione ed educazione dei giovani a livello europeo e internazionale.

Dal 24 al 25 novembre si è tenuto a Buenos Aires il "*Seminario internacional de Centrales de Información y Protección de los Datos Personales*" (Seminario internazionale sulle Centrali rischi e la protezione dei dati personali) organizzato dalla Banca Centrale della Repubblica argentina. Il Presidente Pizzetti ha rappresentato il Garante italiano con un intervento sulla "*Protezione dei dati personali nell'Unione europea*".

21.4. LE MANIFESTAZIONI E LE CONFERENZE

L'attività dell'Autorità collegata a seminari, convegni ed altre iniziative a carattere divulgativo ha visto, nel corso del 2010, la conferma di un grande interesse da parte del pubblico intervenuto. Il Garante ha assicurato la sua presenza ad importanti manifestazioni con il proprio *stand* e con la partecipazione dei suoi rappresentanti a dibattiti.

A gennaio il Servizio relazioni con i mezzi di informazione si è occupato dell'organizzazione della quarta "*Giornata europea della protezione dei dati personali*" che ricorre il 28 gennaio di ogni anno. L'iniziativa, che dal 2007 viene celebrata in tutta Europa con il sostegno della Commissione europea e di tutte le autorità preposte alla protezione dei dati nei Paesi europei, è volta a sensibilizzare i cittadini sulla dignità, sui diritti e sulle libertà fondamentali da salvaguardare rispetto all'uso delle informazioni di carattere personale.

Nel 2010 l'Autorità ha celebrato l'evento con un progetto rivolto alle scuole per sensibilizzare i giovani –attraverso un linguaggio a loro vicino come quello cinematografico–

sul valore della protezione dei dati personali nella società contemporanea e sulla necessità di tutelare la propria vita privata, soprattutto in rete.

L'iniziativa denominata "*Cinema & Privacy: al cinema dal Garante*" ha previsto –a partire dal 28 gennaio e fino al 2 febbraio presso la Sala convegni dell'Autorità– quattro mattine di proiezioni di film che hanno affrontato il tema della *privacy* sotto diversi aspetti. Alle proiezioni hanno partecipato gli studenti di alcune scuole superiori della capitale chiamati dall'Autorità a discutere e confrontarsi.

Si è iniziato con "*Gattaca*", che affronta il tema dell'uso dei dati genetici, per passare a "*La finestra sul cortile*", sul tema del voyerismo, a "*Le vite degli altri*", che tratta il tema del controllo totalitario, e finire con "*Minority report*", su un futuro dominato dalla tecnologia e dai sistemi di sorveglianza.

Ciascun film è stato introdotto da uno dei quattro componenti il Collegio del Garante e da un video appositamente realizzato dal Servizio relazioni con i mezzi di informazione per raccontare, con l'aiuto del cinema, le piccole e grandi "invasioni" della nostra sfera privata.

Dal 17 al 20 maggio, con lo *stand* in parte riprogettato, il Garante ha partecipato alla XXI edizione del *Forum Pa*, importante manifestazione fieristica e congressuale interamente dedicata alla p.a. Il presidente Pizzetti ha introdotto e coordinato il convegno "*La buona trasparenza*" al quale è intervenuto il ministro Brunetta, ed è stato relatore al convegno "*Le Autorità indipendenti e l'economia*". Nell'ambito delle "*Officine p.a.*", il vicepresidente Chiaravalloti ha tenuto un seminario dedicato alla "*Protezione dei dati personali in ambito sanitario*", con particolare attenzione alla sanità elettronica. Il seminario sul "*Potenziamento del ruolo del cittadini nei confronti della p.a.*" è stato tenuto dal componente dell'Autorità Giuseppe Fortunato.

Durante i quattro giorni della manifestazione, stando ai dati forniti dagli organizzatori, è stato registrato un afflusso di circa 42.000 visitatori (circa 15% in più rispetto allo scorso anno) e, come lo scorso anno, un significativo numero di cittadini ed operatori, stimato in una media giornaliera di 650 utenti, ha visitato lo *stand* dell'Autorità dove erano in distribuzione le pubblicazioni curate dall'Ufficio, in particolare il nuovo *vademecum* dedicato alla *privacy* nella scuola, l'opuscolo sull'uso consapevole dei *social network* e la

brochure illustrativa del nuovo *provvedimento* generale sulla videosorveglianza, disponibile anche in lingua inglese. A disposizione del pubblico anche la XX edizione del *Dvd* "*Il Garante e la protezione dei dati personali*".

Dal 10 al 13 novembre, l'Autorità ha partecipato alla XXVII Assemblea annuale dell'ANCI organizzata presso il quartiere fieristico di Padova. Nell'ambito della manifestazione il presidente Pizzetti è intervenuto alla presentazione delle "*Linee-guida in materia di videosorveglianza*" messe a punto dall'ANCI sulla base del *provvedimento* generale adottato dal Garante nell'aprile 2010, sottolineando l'importanza della collaborazione istituzionale in settori tanto delicati come quello della sicurezza, anche alla luce delle nuove tecnologie di raccolta, elaborazione e conservazione dati oggi a disposizione.

21.5. LE RELAZIONI CON IL PUBBLICO

Nel 2010 l'Autorità ha confermato il suo importante ruolo nella difesa dei diritti della persona anche nel rapporto fra pp.aa., caratterizzando il servizio prestato con disponibilità ed elevati *standard* qualitativi, in linea con il principio di trasparenza amministrativa introdotto dalla l. 7 agosto 1990, n. 241, attraverso l'uso di canali comunicativi contraddistinti da efficacia, accuratezza, rapidità per realizzare un modello di contiguità fra persone e amministrazione.

L'attività dell'URP, improntata all'efficienza ed alla contestualità fra sollecitazioni ricevute e risposte fornite, consente una costante verifica dell'efficacia dell'attività dell'Autorità in termini di soddisfazione del cittadino, attraverso la circolarità del flusso che dalle numerosissime sollecitazioni dell'utenza si produce con i singoli provvedimenti dell'Autorità.

La partecipazione del cittadino all'attività amministrativa si esplica attraverso la collaborazione del personale dell'Ufficio, che favorisce il costante aggiornamento sull'evoluzione procedimentale inerente a singole posizioni e fornisce chiarimenti in merito alle tematiche complesse sottoposte alla sua attenzione.

Altrettanto rilevante è la funzione comunicativa che l'Ufficio svolge nei confronti dell'intera compagine dell'Autorità, attraverso un'attenta disamina delle istanze relative a

questioni verso le quali la comunità mostra particolare sensibilità, allo scopo di accrescere l'efficacia dell'attività dell'Amministrazione.

L'attività dell'Ufficio relazioni con il pubblico

L'attività dell'URP si fonda sempre più sull'elaborazione in tempo reale delle diverse istanze proposte dai cittadini, che consente la razionalizzazione delle problematiche più rilevanti e lo sviluppo dinamico delle soluzioni offerte, spesso anche contestualmente, nei confronti di più sollecitazioni. L'esaustività delle informazioni fornite, la loro immediatezza e la flessibilità della prestazione vengono riconosciute dall'utenza come tratti distintivi e qualificanti del servizio prestato.

Le articolate funzioni dell'Ufficio sono riconducibili a tre grandi aree:

- semplificazione: mediante la compilazione di modelli di istanza mirati e di note tipo, l'Ufficio assiste il singolo cittadino nell'individuazione della tipologia di strumento di tutela predisposto dal Codice, dopo un approfondimento della tematica di interesse mediante la documentazione messa a disposizione dall'Autorità;
- comunicazione e gestione integrata dei rapporti con l'utenza: attraverso la raccolta delle segnalazioni e delle sollecitazioni viene realizzato un flusso divulgativo circolare che consente di indirizzare gli interventi sulle tematiche di maggiore interesse, dando poi rilievo alle medesime problematiche attraverso la divulgazione dell'attività dell'Autorità;
- informazione al cittadino: l'attività si esplica mediante rapporto diretto e dedicato presso la sede istituzionale oppure mediante gli strumenti di comunicazione ordinari (contatto telefonico o posta elettronica).

Risulta inoltre particolarmente richiesta ed utile l'attività di assistenza alla navigazione all'interno del sito dell'Autorità.

In virtù dell'ottimizzazione delle attività appena enunciate, anche nel trascorso anno di attività, l'Ufficio ha ricevuto considerevoli attestazioni di gradimento del servizio erogato, confermando il positivo riscontro ottenuto dai cittadini nei confronti dell'impegno di contenuto anche formativo (rapporto "*qualità erogata*" e "*qualità percepita*").

La grande risonanza che i mezzi di informazione conferiscono ad alcune particolari vicende che riguardano la sfera della riservatezza delle persone comporta un considerevole

incremento delle richieste di chiarimenti ed approfondimento, talvolta con espressione di opinioni critiche da parte degli utenti.

Anche in seguito alle tempestive reazioni della pubblica opinione alle sollecitazione dei *media*, il Garante interviene con grande frequenza in merito al trattamento dei dati personali nell'ambito dell'attività giornalistica, stigmatizzando prassi scorrette e lesive dei diritti riferiti non solo a persone note, oggetto di abusi nella loro vita quotidiana, ma soprattutto a soggetti socialmente deboli ed esposti, quali malati, minori, vittime di reati o sottoposti ad indagini giudiziarie.

Già da una prima analisi delle istanze pervenute, risulta evidente la sensibilità dei cittadini in merito al *direct marketing*, con particolare riferimento a quello telefonico, in considerazione dell'invasività e della massività dell'attività in questione. In vista dell'entrata in vigore delle recenti novità normative (d.P.R. 7 settembre 2010, n. 178 "*Regolamento recante istituzione e gestione del registro pubblico degli abbonati che si oppongono all'utilizzo del proprio numero telefonico per vendite o promozioni commerciali*", in *G.U.* 2 novembre 2010, n. 256), l'attenzione dell'utenza si è focalizzata sull'efficienza dell'impianto normativo vigente, oltre che sulle aspettative e, in qualche caso, sulle perplessità in merito al sistema dell'"*opt out*" in materia di consenso preventivo per il ricevimento di messaggi a contenuto pubblicitario.

L'Ufficio ha al riguardo svolto una rilevante attività di chiarimento ed aggiornamento sul quadro normativo vigente, anche nel periodo transitorio.

Le numerosissime sollecitazioni relative a telefonate pubblicitarie indesiderate hanno comportato un rilevante impegno sia per l'informazione sulle norme applicabili, sia per l'assistenza nell'individuazione dello strumento di tutela più opportuno in ragione del singolo caso in esame.

Con riferimento alle diverse tipologie di quesiti e di argomenti, anche attraverso la reiterazione dei contatti con l'utente, l'URP esplica un'assistenza continuativa a partire dalla valutazione dei presupposti dell'azione sino al materiale inoltro dell'istanza formale presso l'Autorità, con riguardo alla sussistenza dei requisiti formali e sostanziali per l'intervento dell'Autorità attraverso il dipartimento competente. Il ruolo di informazione nei confronti del cittadino istante persiste nel corso dello sviluppo del procedimento amministrativo,

arricchendosi di ulteriori apporti di chiarimento e integrazione, che vanno dalla semplice richiesta di conoscere lo stato del procedimento alla richiesta di accesso agli atti ai sensi della l. n. 241/90, ecc.

L'esame dei dati statistici relativi all'attività dell'URP conferma l'elevato livello di attenzione manifestato dall'utenza in merito alle problematiche connesse alla protezione dei dati. Nell'ambito dell'attività di *front office*, infatti, i contatti registrati nel periodo di riferimento sono pari a 26.243 (contatti telefonici, e-mail, visitatori, fascicoli), di cui 25.377 avvenuti a mezzo del telefono e della posta elettronica. A questi dati vanno aggiunti 295 fascicoli trattati nel corso del 2010.

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 12.767.

Gli utenti hanno comunque manifestato gradimento anche per attività di ricevimento dei visitatori, conteggiati in circa 571 unità: laddove possibile, questa modalità di contatto consente la consegna di materiale informativo che attribuisce ulteriore funzionalità all'attività di assistenza.

L'Ufficio ha ricevuto inoltre 12.610 quesiti per e-mail e posta ordinaria: la trattazione di essi è avvenuta nella gran parte dei casi in tempi notevolmente celeri (uno o due giorni lavorativi), anche per garantire, oltre alla qualità, tempestività della risposta.

L'analisi dei dati elaborati dall'Ufficio consente peraltro la valutazione non solo della tipologia delle richieste ma anche della variegata composizione dell'utenza. In ragione della provenienza dell'istanza, quindi, l'Ufficio elabora un *output* adeguato all'esperienza dell'istante, sia esso un privato, un soggetto pubblico, un consulente dotato di competenze avanzate.

È stato peraltro possibile osservare che un certo numero di utenti stabilisce un rapporto continuativo con l'Ufficio: frequentemente, infatti, al primo contatto ne seguono altri, funzionali all'approfondimento della normativa e dei provvedimenti dell'Autorità, realizzando con questa modalità un approccio dinamico ed esaustivo delle problematiche sottoposte all'attenzione dell'Autorità.

In questi specifici casi la tempestività e l'efficienza del supporto prestato risultano di primaria importanza per il buon esito del servizio e per l'affinamento delle procedure interne.

In particolare l'Ufficio riserva attenzione particolare allo sviluppo di procedure per la gestione delle emergenze, garantendo il coinvolgimento immediato dei dipartimenti competenti e dei vertici istituzionali secondo necessità.

Tematiche d'interesse

L'esame dei dati elaborati dall'Ufficio consente di esaminare le tematiche più ricorrenti, oggetto di attenzione da parte di cittadini e p.a.

Il trattamento dei dati personali nell'ambito dell'attività di *marketing* si conferma, come accennato, di grande interesse per gli utenti, sia per la corretta predisposizione di procedure ed adempimenti da parte degli operatori del settore, sia per il gran numero di comunicazioni pubblicitarie indesiderate, attraverso strumenti di vario genere (telefonate, fax, e-mail, *Sms*).

Inoltre pervengono costantemente molteplici richieste di intervento relativamente all'attività di *spamming* via e-mail ed all'inoltro massivo di fax pubblicitari indesiderati o anche solo a tentativi di trasmissione fastidiosamente ripetuti. In tale settore l'Ufficio ha anche svolto un'attività di verifica dei presupposti delle violazioni, formulando spesso richieste di integrazione, così consentendo l'avvio di numerose istruttorie in ordine a questa particolare forma di pubblicità, percepita frequentemente come invasiva e molesta.

Considerevole interesse è stato suscitato dal *provvedimento* generale in materia di videosorveglianza (8 aprile 2010 [doc. *web* n. 1712680]), con particolare riferimento ai casi in cui detta attività viene posta in essere dai privati cittadini per finalità esclusivamente personali ed alle ipotesi in cui essa si combini con altri sofisticati strumenti di controllo nell'ambito dell'attività lavorativa dipendente. Nello stesso contesto, numerose richieste di chiarimento riguardano la liceità dell'uso della biometria in ambito lavorativo.

Anche in virtù dei numerosi interventi e richiami dell'Autorità in merito al trattamento dei dati personali nell'ambito dell'attività giornalistica, risultano essere molto numerose le richieste di chiarimenti. Come già negli anni precedenti, la capillare diffusione delle testate giornalistiche *online* ha comportato la necessità di fornire chiarimenti in merito al corretto esercizio del diritto di cronaca ed al diritto all'oblio in Internet, oltre che riguardo agli strumenti di tutela adeguati ai singoli casi.

Il massivo ricorso dei nuovi strumenti di comunicazione ha evidenziato l'esigenza di protezione dei dati personali all'interno dei "*social network*" (ad es., *Facebook*, *MySpace*), non solo da parte degli utenti di giovane età, soprattutto attraverso la ricerca di adeguati strumenti di tutela nella normativa vigente.

Le problematiche relative al trattamento dei dati in ambito lavorativo sono costantemente all'attenzione dell'Ufficio, con riferimento al tema della trasparenza nelle amministrazioni pubbliche (cartellini identificativi; retribuzioni e *curricula* dei dirigenti; tassi di assenza e di maggiore presenza del personale).

È inoltre costante l'interesse per il trattamento dei dati personali in ambito bancario e, più in generale, del credito e degli investimenti. Le richieste di chiarimenti e di intervento in relazione alla corretta gestione del rapporto con i clienti hanno riguardato anche problematiche sorte negli ultimi anni in relazione all'entrata in vigore di norme volte alla valutazione dell'adeguatezza e dell'appropriatezza delle operazioni o dei diversi servizi di investimento forniti (Direttive nn. 2004/39/CE e 2006/73/CE), nonché in relazione all'adozione della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231).

Ancor più ricorrenti sono state le richieste di assistenza per attivare le procedure di intervento a correzione delle informazioni personali trattate da parte dei sistemi informativi privati in materia di credito al consumo e puntualità e affidabilità nei pagamenti.

Un aspetto dell'attività dell'URP da menzionare è infine la divulgazione del materiale informativo predisposto dall'Autorità. In occasione dell'afflusso di pubblico presso la sede del Garante o mediante richieste a distanza, l'Ufficio distribuisce secondo princìpi di efficacia e razionalizzazione la documentazione disponibile sui diversi argomenti di interesse dell'utenza.

21.6. IL SERVIZIO STUDI E DOCUMENTAZIONE

La redazione della *Relazione* annuale

In conformità alle proprie competenze il Servizio studi ha coordinato la redazione del testo della *Relazione* annuale al Parlamento, avvalendosi, come di consueto, della preziosa collaborazione della redazione *web*.

Tale adempimento, oltre a costituire un fondamentale compito istituzionale dell'Autorità, rappresenta, come più volte già segnalato in questa sede, un'importante occasione di

bilancio e riflessione sull'attività svolta nel corso dell'anno, anche per ciò che attiene a possibili miglioramenti nello svolgimento delle funzioni istituzionali e nel rendere conoscibile l'attività del Garante non solo ai soggetti più direttamente interessati, ma in termini più generali ai cittadini.

La funzione di studio e di supporto giuridico

Il Servizio studi ha continuato a svolgere attività di studio e ricerca su questioni tecnico-giuridiche di interesse dell'Autorità anche su impulso del Collegio, del segretario generale nonché delle strutture dell'Ufficio.

Si cita al riguardo, a titolo meramente esemplificativo, l'approfondimento di tematiche riguardanti la determinazione della legge applicabile al trattamento di dati personali, in casi che presentino connessioni con più di un ordinamento giuridico. Trattasi di tema particolarmente complesso per la molteplicità di profili sostanziali e processuali anche di natura comunitaria, oggetto di discussione in sede di Gruppo Art. 29 ed esaminato nella prospettiva di eventuali modifiche della Direttiva n. 95/46/CE.

La problematica della trasparenza nella *cd.* "amministrazione digitale" è stata considerata in un parere interno avente ad oggetto la legittimità della diffusione *online* dei bollettini ufficiali delle amministrazioni pubbliche, specie con riferimento ai dati personali dei dipendenti relativi a sanzioni disciplinari, alla responsabilità verso l'amministrazione e i terzi, nonché all'invalidità per causa di guerra o di lavoro e alle infermità contratte per causa di servizio. Questo in un contesto normativo caratterizzato dal susseguirsi, in termini non sempre chiarissimi, di previsioni normative e contrattuali, da leggere alla luce delle disposizioni contenute nel Codice (cfr. art. 24, commi 1 e 3, d.P.R. 3 maggio 1957, n. 686; artt. 17, comma 2, e 34, comma 2, CCNL Ministeri 16 maggio 2001).

Si menziona ancora, oltre ad un approfondimento relativo allo svolgimento dei poteri propri del Garante, in relazione all'impugnazione di atti istruttori, una questione riguardante l'ambito di applicazione del diritto di accesso previsto nella l. n. 241 del 1990, in un caso in cui l'istanza appariva diretta a ricostruire il comportamento di soggetti terzi che, come l'istante, erano stati parti di un pregresso e definito procedimento del Garante. Si è trattato, conformemente al ruolo e alle competenze del Servizio studi, di una valutazione relativa non al merito dell'istanza ossia ai profili di fatto, ma, alla luce

degli orientamenti giurisprudenziali e dottrinali, alla sussistenza dell'interesse all'accesso in capo al richiedente, in una situazione che si può presentarsi non infrequentemente presso l'Autorità.

Il Servizio studi ha inoltre costantemente coadiuvato l'attività istituzionale del Garante attraverso la ricerca e la fornitura alle strutture interessate di documentazione nazionale ed internazionale nonché di sintetiche osservazioni su questioni d'interesse per l'Autorità quali, nel periodo in esame, Internet e *copyright*, pedofilia e protezione dati, autorità indipendenti sulla protezione dati in Europa.

I pareri sulle leggi regionali

Il Servizio ha altresì costantemente fornito elementi di valutazione per i pareri richiesti dalla Presidenza del Consiglio dei ministri, ai fini dell'eventuale impugnazione davanti alla Corte costituzionale ai sensi dell'art. 127 della Costituzione. Trattasi, come più volte riferito in precedenti edizioni della *Relazione*, di un atto interno volto a valutare la conformità delle leggi regionali alla normativa nazionale e comunitaria sulla protezione dei dati personali.

Risulta allo stato stabilizzata la tendenza, costantemente registrata da alcuni anni, al rispetto dei limiti costituzionali di cui all'art. 117, anche alla luce di quanto stabilito dalla Corte costituzionale sulla competenza legislativa esclusiva dello Stato in materia di *privacy* (cfr. sentenza n. 271/2005).

In tale quadro, oltre a taluni aspetti relativi a possibili profili di incostituzionalità che l'Autorità ha segnalato alla Presidenza del Consiglio (v. par. 1.3.), si segnalano alcune criticità riguardanti una legge regionale in materia sanitaria, in relazione ad una previsione relativa alla pubblicazione dei ruoli del personale, che, nel riferimento ai dati matricolari dei dipendenti, ha suscitato perplessità circa il mancato rispetto del principio di pertinenza, evidenziando la complessa tematica dell'impugnabilità di norme legislative sulla base di interpretazioni possibili, purché non implausibili ovvero scollegate dalle disposizioni impugnate.

Ulteriori approfondimenti sono stati svolti con riguardo ad una legge regionale relativa all'istituzione del bollettino ufficiale telematico recante, salve le esigenze di riservatezza, il principio della integrale pubblicazione di alcuni atti amministrativi quale forma di

soddisfacimento del diritto di accesso. In proposito si è evidenziato che la mancanza delle garanzie procedimentali previste in materia di accesso dalla legge statale parrebbe idonea ad abbassare la soglia di tutela prevista dalla normativa statale, in possibile contrasto con i princìpi costituzionali del riparto della competenza legislativa tra Stato e Regioni di cui all'art. 117.

Si citano infine le previsioni di una legge provinciale, che disciplina in termini relativamente ampli la pubblicazione di dati dei dipendenti pubblici, esaminate alla luce di norme e princìpi comunitari per verificare se potesse configurarsi un'ingerenza nella vita privata non compatibile con l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo (CEDU).

I servizi interni di documentazione

Il Servizio studi ha infine continuato a curare l'aggiornamento del personale anche 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, letteratura 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, specificamente mirate ad importanti ambiti di attività del Garante quali quelli in materia di libertà pubbliche e sanità, comunicazione e reti telematiche, realtà economiche e produttive, amministrazione, contratti e risorse umane; il "*Servizio studi news*", uno strumento informativo che si prefigge di segnalare tempestivamente all'Ufficio soprattutto le novità giurisprudenziali, anche attraverso l'utilizzo di fonti giornalistiche, in materia di diritti e libertà delle persone e protezione dei dati personali, che costituisce un proficua occasione di monitoraggio ed approfondimento dei profili comunitari ed internazionali in un materia che si caratterizza sempre di più per l'applicazione, da parte di autorità e giudici diversi, di princìpi comuni (v., ad es., la decisione della CEDU 18 gennaio 2011, nel caso *Mgn Limited v. The United Kingdom*, ricorso n. 39401/04, in *http://www.echr.coe.int/echr/Homepage_EN*, e quella della Corte di Giustizia dell'Unione europea 9 novembre 2010, in C-92/09 e 93/09, riunite (*Volker und Markus Schecke GbR, Hartmut Eifert*), in *http://curia.europa.eu/*).

21.7. LA BIBLIOTECA

La Biblioteca nasce nel 2001 ed è un'unità di 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 di legge, l'incremento del patrimonio della biblioteca si estende alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale. Un ulteriore campo di sviluppo è costituito dalla storia della vita privata nell'età moderna e dalle matrici storico-religiose del *right to privacy*. In collaborazione con il Dipartimento risorse tecnologiche è stato poi creato un fondo speciale di testi scientifici sulle tecnologie dell'informazione in rapporto alla protezione dei dati.

Attualmente la Biblioteca possiede circa 9.500 volumi (circa 5.500 in lingua straniera), 400 testate di periodici e 200 testi di laurea e di dottorato.

Nel corso del 2010 è proseguito il progetto di ampliamento del patrimonio, con la raccolta delle pubblicazioni a stampa di tutte le autorità di protezione dei dati in Europa e nel mondo. È continuato lo spoglio sistematico dei titoli analitici in materia di protezione dei dati che appaiono su monografie e periodici italiani e stranieri: questo settore di acquisizione si avvale di *database online* che facilitano, in particolare, il monitoraggio dei periodici giuridici di lingua inglese.

La necessità di riordinare sulla base di nuovi criteri il vasto patrimonio bibliografico raccolto nell'arco di un decennio è all'origine della preparazione di due documenti specifici quali la Carta delle collezioni e il *Regolamento*. La prima descrive gli indirizzi per l'incremento del posseduto, evidenziando con precisione i settori disciplinari presenti in catalogo e indicando le aree di possibile espansione. Il secondo definisce gli scopi e le modalità di funzionamento della Biblioteca, principalmente per quanto concerne l'utenza interna.

Il progetto di *Digital Library*, avviato nel 2008 in cooperazione con il Dipartimento risorse tecnologiche, costituisce una priorità del programma di riorganizzazione. Accanto alle "strategie di possesso" (imperniate sull'aumento del patrimonio cartaceo) sono state delineate nuove "strategie di accesso" concentrate sull'acquisizione di archivi pubblicati in

formato elettronico. Il sito *web* della Biblioteca, trasformato in portale, è stato suddiviso in aree funzionali in modo da coordinare tutte le risorse bibliografiche elettroniche (l'*OPAC online* e i *database*) nel quadro di una *knowledge infrastructure*: questa architettura di conoscenze condivise supporta le attività di studio e di ricerca intraprese dalla presidenza e dai componenti del Collegio e, in parallelo, fornisce una serie di strumenti informativi qualificati per le attività dei dipartimenti e dei servizi nei rispettivi settori di competenza.

L'infrastruttura elettronica ha ricevuto nuovo impulso dall'ampliamento dei moduli dei *database* (con incremento esponenziale della documentazione *full-text*) e dall'inserimento della formula della multiutenza sulla rete intranet. Questo dispositivo tecnico ha permesso di ottimizzare le risorse, aumentando il numero delle banche dati giuridiche di accesso *web* e di accesso remoto rese disponibili su tutte le postazioni dell'Ufficio.

Nel 2010 le richieste di titoli in lettura da parte di utenti interni sono state 4.500 (+7% sul 2009): le domande di frequentazione di utenti esterni assommano a 255 (+2% sul 2009), con circa 1850 richieste di titoli in lettura. I contatti sul catalogo *OPAC* sono stati 6.500.

I dati analitici relativi alla consultazione dei *database* appaiono in sintonia con il *trend* di forte crescita già segnalato nel 2009. Per quanto riguarda le tre banche dati giuridiche di maggiore rilevanza il numero globale delle sessioni è stato di 4.893 (con una media mensile di 407). Il *database* che registra il più elevato conteggio statistico totalizza 4.052 sessioni di lavoro e 48.112 documenti consultati, pari a una media mensile di 337 sessioni e 4.009 documenti (+6% sul 2009).

21.8. LE ALTRE INIZIATIVE DI COMUNICAZIONE E RICERCA

21.8.1. Il Laboratorio Privacy Sviluppo

Si è riferito nelle relazioni degli anni scorsi del *Laboratorio Privacy Sviluppo*, nato con il favore del Collegio e coordinato dall'Avv. Giuseppe Fortunato. Accanto all'attività istituzionale dell'Autorità, il Laboratorio si occupa dell'altra faccia della *privacy*: la libera costruzione della propria sfera privata e il pieno esercizio della "sovranità su di sé".

Quest'anno si sono ampiamente sviluppate le ricerche sul testo "*LA SVOLTA. Dal desiderio alla realtà*", argomento di nuove tesi di laurea non solo in discipline filosofiche, psicologiche, sociologiche e giornalistiche, ma anche storico-artistiche presso l'Accademia delle Belle Arti.

È nato ad opera di artisti un apposito gruppo "*Artivismo Civicratico*" che si ispira a tali ricerche, per operare in ambito artistico e sociale.

Sono proseguiti seminari, in particolare nelle scuole e nelle università (LUMSA, La Sapienza, Cattolica Università di Bari) e presso centri culturali.

Il gruppo di giovani studenti che ha dato vita ad un ciclo di seminari denominati "*Gli Argonauti de LA SVOLTA*" ha sviluppato le sua attività, approntando una particolare modalità interattiva (l'anticorso).

A seguito di tali seminari è stato nuovamente aggiornato il Quesitario de LA SVOLTA, sempre aperto a nuovi contributi.

Oltre alla collaborazione con la Commissione Europea, sono state avviate ulteriori collaborazioni internazionali con ONU e Consiglio d'Europa.

Il Comitato Nazionale Emittenti televisive Locali, aderente al Laboratorio, ha costruito un apposito format televisivo (CIVINEWS) che si è sviluppato in sei diverse puntate ed ha avuto ampia diffusione su testate televisive locali. Tali iniziative sono state caratterizzate, nello spirito de LA SVOLTA, dalla comunicazione di "*good news*" ossia esempi di buona attività, sovente effettuate da associazioni e gruppi volontari.

Grazie alla cooperazione del Ministero dei beni culturali, LA SVOLTA è stata presentata con successo al Salone Internazionale del Libro di Francoforte.

Si sono sviluppati i rapporti con categorie professionali in appositi incontri loro dedicati (in particolare: giornalisti, psicologi, avvocati, difensori civici, segretari comunali, revisori legali) da cui hanno avuto origine proficui rapporti di collaborazione, in diversi casi sulla base di convenzioni stipulate con ordini e organismi.

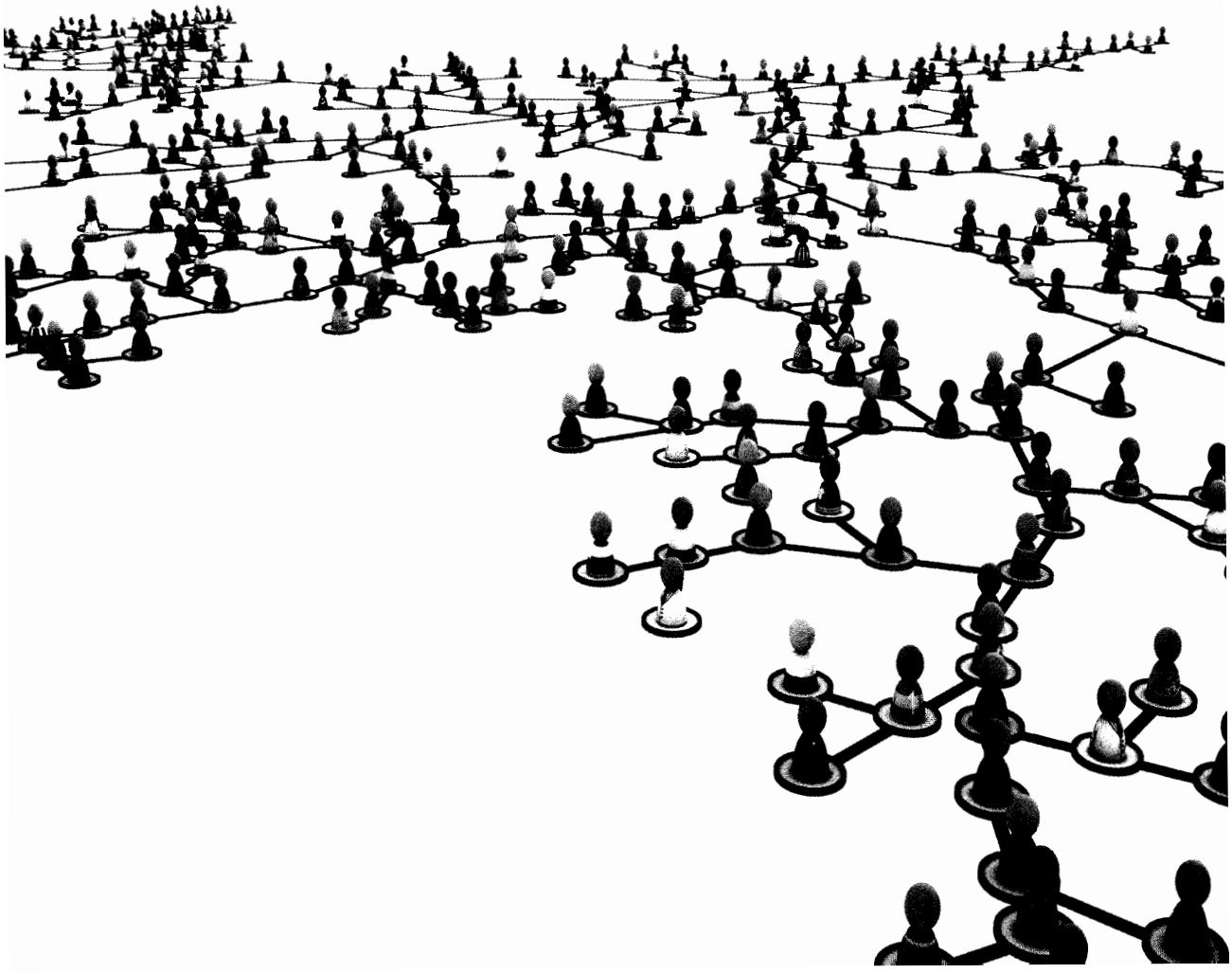
Sulla base del Manifesto elaborato da Civicrazia, già segnalato nella relazione dello scorso anno, è stato altresì elaborato un Decalogo per il comune civicratico, improntato a trasparenza, efficienza dei servizi pubblici, meritocrazia e celere tutela dei diritti dei cittadini.

Sulla base degli stessi princìpi, al *Forum Pa* è stato presentato un "*Vademecum del comune delinquente telematico*", con il quale sono state sinteticamente indicate alcune violazioni della normativa sulla *privacy* commesse da amministrazioni comunali.

Il *Vademecum*, in dieci punti sulla base dell'acrostico T.E.L.E.M.A.T.I.C.O., è stato molto gradito, per il suo taglio pratico, da diversi operatori del *web*, i quali si sono prontamente impegnati a divulgarlo per consentire di riconoscere e contrastare i "delinquenti telematici".

Il Laboratorio, sempre più punto di riferimento per associazioni e organismi, è costantemente impegnato nella realizzazione di molteplici attività di studio e di ricerca incentrate sulla tutela e lo sviluppo della persona, perché la scoperta e l'affermazione di sé stessi rappresentano il viaggio più complesso, ma anche il più affascinante, da realizzare.

L'Ufficio del Garante



PAGINA BIANCA

III. L'Ufficio del Garante

22. La gestione amministrativa dell'Ufficio

22.1. Il bilancio, gli impegni di spesa e l'attività contrattuale

Le risorse finanziarie acquisite al bilancio del Garante sono state utilizzate per le esigenze gestionali volte al perseguimento delle finalità istituzionali e dei compiti affidati all'Autorità, nonché per gli obiettivi programmatici definiti in sede di approvazione del bilancio di previsione per il 2010, nel rispetto delle procedure di legge e regolamentari che disciplinano la materia.

La gestione amministrativa dell'Ufficio ha fatto registrare nell'esercizio 2010 un incremento delle entrate complessive di competenza in misura pari a circa 1,3 milioni di euro, per un totale di 16,6 milioni di euro.

La voce più significativa delle entrate ammonta a 13,4 milioni di euro (pari all'80,7% del totale) ed è rappresentata dal contributo erogato a carico del bilancio dello Stato, la cui misura, ancorché ridotta rispetto al maggiore stanziamento iniziale previsto dalla Legge finanziaria del 2010, appare sostanzialmente in linea con i trasferimenti assicurati nel precedente esercizio (13,4 milioni di euro del 2010 rispetto a 13,1 milioni di euro del 2009).

Entrate più che doppie rispetto al precedente esercizio sono state assicurate dai proventi derivanti dalle sanzioni pecuniarie affluite al bilancio del Garante, il cui importo per il 2010 è di poco inferiore ai 2 milioni di euro (a fronte di 0,8 milioni di euro del 2009) e corrisponde al 50% delle somme complessivamente affluite al bilancio dello Stato, per il quale l'Autorità ha titolo al rimborso (art. 166 del Codice).

Tale variazione, significativa in termini percentuali, si inserisce in un *trend* di crescita che ormai si registra da alcuni anni. Tuttavia, in valore assoluto rappresenta ancora un'entità limitata rispetto alle entrate complessive occorrenti all'Autorità per fare fronte alle spese complessive necessarie al proprio corretto funzionamento e, in prospettiva futura, non appare ipotizzabile il ricorso ad ulteriori incrementi di tale fonte di finanziamento.

Per quanto riguarda la spesa, le finalità istituzionali dell'Autorità sono state perseguite nel rispetto dei vincoli di bilancio e degli indirizzi di contenimento previsti dalle disposizioni legislative intervenute in materia.

La spesa complessiva imputabile alla competenza dell'esercizio ammonta a 17,7 milioni di euro, la cui entità fa registrare una contrazione significativa rispetto al precedente esercizio, anche se il rallentamento della spesa resta influenzato non solo da politiche di contenimento e di razionalizzazione, che comunque sono state poste in essere, ma da spese di natura straordinaria sostenute nel 2009 che non si sono ripresentate nel 2010.

Ciò nonostante, la gestione amministrativa dell'esercizio determina un disavanzo di competenza di 1,1 milioni di euro alla cui copertura finanziaria si è provveduto attraverso l'utilizzo di una parte delle economie realizzate negli anni pregressi, così evitando di ridimensionare l'attività amministrativa dell'Autorità.

Per la parte più significativa della spesa, avente carattere fisso e continuativo, non si ravvisano particolari margini di intervento.

La rimanente parte della spesa, connessa essenzialmente al funzionamento dell'Autorità, assume valore meno rilevante e la sua entità complessiva è ricondotta entro i limiti previsti dalle disposizioni finanziarie di contenimento della spesa pubblica adottate dal legislatore.

Le spese di investimento durevole, di entità poco significativa rispetto all'ammontare delle spese complessive, evidenziano una riduzione rispetto al precedente esercizio.

L'ultima tabella allegata alla presente Relazione riassume sinteticamente i valori finanziari di competenza che hanno interessato la gestione dell'Autorità nel 2010, posti a raffronto con quelli dell'esercizio precedente.

In particolare, sono esposte le fonti di finanziamento dell'Autorità, con evidenziazione delle somme poste a carico del bilancio dello Stato, nonché la spesa complessiva dell'esercizio di riferimento, per la quale l'onere degli interventi in conto capitale è esposto separatamente rispetto alla spesa per il funzionamento.

Una colonna a parte, infine, evidenzia gli scostamenti registrati nell'anno rispetto agli analoghi valori del periodo precedente.

La gestione amministrativa, pur nel rispetto dei vincoli di bilancio dettati dalle disposizioni legislative in materia, è stata indirizzata ad un generale miglioramento delle funzionalità operative dell'Ufficio, con particolare riferimento al potenziamento dei settori strategici nei quali si esplica l'attività dell'Autorità.

Nello svolgimento dell'attività di controllo, la struttura ha continuato ad avvalersi di personale dipendente dal corpo della Guardia di finanza in servizio presso l'Ufficio del Garante, che ha affiancato il personale in organico, ed è proseguita la collaborazione con il Nucleo speciale funzione pubblica e *privacy* della Guardia di finanza.

L'attività contrattuale

Per quanto attiene all'attività contrattuale, nel 2010 l'Ufficio ha perseguito anzitutto l'obiettivo di assicurare un elevato livello di servizi alle unità organizzative, con oneri invariati, ovvero in taluni casi decrescenti, attraverso un processo di razionalizzazione e riqualificazione della spesa.

A tal fine, è stato incrementato il ricorso alle procedure di acquisizione di beni e servizi mediante centrale di acquisto (CONSIP S.p.A.), e soprattutto attraverso il mercato elettronico della p.a., che ha consentito un miglioramento sia in termini di efficienza, sia di snellimento e trasparenza delle procedure.

Nell'ambito delle aree che hanno interessato la prevalente attività contrattuale dell'Ufficio –risorse tecnologiche, relazioni con i *media* e attività di manutenzione della sede– sono state avviate alcune procedure comparative volte al miglioramento dei servizi per l'utenza, nonché ai necessari aggiornamenti tecnologici e di sicurezza delle componenti *hardware* e *software* in dotazione.

Merita di essere segnalata, tra le altre, la procedura relativa al rifacimento completo del sito *web* del Garante, finalizzata ad una maggiore chiarezza ed accessibilità dei contenuti, allo sviluppo di nuove funzionalità di gestione e ad un indispensabile aggiornamento sotto il profilo della sicurezza informatica.

Riguardo al funzionamento dell'Ufficio, sono stati attuati significativi risparmi di spesa mediante la riduzione e razionalizzazione del servizio di trasporto con conducente, anche in questo caso all'esito di una procedura comparativa.

Va infine segnalato il costante aggiornamento richiesto per lo svolgimento dell'attività

negoziale, oggetto di ulteriori e significative novità normative –quali, a titolo esemplificativo, le modifiche al codice dei contratti pubblici recate dal d.lgs. 20 marzo 2010, n. 53, le disposizioni in materia di tracciabilità dei flussi finanziari, nonché l'approvazione del nuovo regolamento di attuazione del citato codice– che richiedono un correlativo aggiornamento delle procedure e del *know-how* dell'Ufficio.

22.2. LE NOVITÀ LEGISLATIVE E REGOLAMENTARI E L'ORGANIZZAZIONE DELL'UFFICIO

Nel corso del 2010 sono state adottate alcune rilevanti decisioni volte al miglior funzionamento dell'Ufficio.

A conclusione di un processo di ricognizione e rivisitazione dell'organizzazione interna, il Garante ha assunto la determinazione di un riassetto complessivo dell'Ufficio, in considerazione delle numerose modifiche normative e degli accresciuti compiti dell'Autorità verificatisi nel corso degli ultimi anni.

In coincidenza con la decisione di nominare segretario generale un dirigente scelto all'interno del ruolo organico del personale, sono stati individuati tre dirigenti con funzioni di vicesegretario generale, al fine di garantire il migliore svolgimento delle attività di coordinamento dell'Ufficio. A tale decisione si è data concreta attuazione nel marzo 2010.

Con la medesima finalità di assicurare un miglior funzionamento dell'Ufficio e di rimodellare alcuni istituti retributivi già previsti in via regolamentare e rimasti in parte inattuati, sono stati sottoscritti nel novembre 2010 tre accordi negoziali con le organizzazioni sindacali del personale, a conclusione di una lunga trattativa.

In particolare, il primo dei citati accordi negoziali persegue l'obiettivo di rimuovere le criticità emerse nell'attuazione dell'istituto delle progressioni economiche biennali mediante circoscritte modifiche ad alcuni profili regolamentari. Ciò al fine di rendere l'istituto meglio rispondente all'esigenza di valorizzare il merito, tenuto conto della presenza, all'interno dell'organico dell'Autorità, di personale con elevata professionalità ed esperienza.

In tale quadro, alla luce delle novità legislative di recente intervenute, considerate le strette interrelazioni esistenti tra il sistema di valutazione e l'istituto delle progressioni

economiche, è apparso opportuno apportare talune modifiche alle pertinenti diposizioni regolamentari in tema di valutazione del personale, all'esito di successivi approfondimenti e di un proficuo confronto con le rappresentanze sindacali del personale.

Nel corso del periodo considerato, pur nel contesto di una sensibile riduzione dello stanziamento a disposizione dell'Autorità, sono proseguite le iniziative per potenziare e consolidare l'organico dell'Ufficio al fine di un migliore svolgimento delle funzioni istituzionali, completando l'immissione in servizio del personale già reclutato e dando concreta attuazione allo scorrimento della graduatoria di merito del concorso pubblico per la qualifica di funzionario con profilo giuridico-amministrativo.

Come si dirà nel paragrafo successivo, è stata altresì indetta una procedura selettiva per completare il contingente di personale assunto con contratto a tempo determinato, fissato legislativamente in venti posti.

L'attività di segreteria del Collegio

Nel corso dell'ultimo anno il Garante ha anche provveduto ad una miglior definizione delle attività facenti capo al Servizio segreteria del Collegio, al fine di migliorarne la funzionalità e l'efficienza.

Con delibera del 9 dicembre 2010, in attuazione di quanto previsto dal regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio, l'Autorità ha disciplinato la redazione del processo verbale delle riunioni del Collegio, in particolare per quanto concerne finalità e utilizzo della registrazione audio e stesura del verbale medesimo.

Per facilitare l'attività interna di documentazione, l'Ufficio ha provveduto all'istituzione di un "registro interno delle deliberazioni collegiali", numerate per agevolare la reperibilità, nonché alla realizzazione dell'archiviazione digitale, istituendo una "cartella elettronica" disponibile sulla rete intranet del Garante e contenente i documenti relativi a ciascuna adunanza del Collegio (ordini del giorno, verbali e documenti approvati).

22.3. IL PERSONALE E I COLLABORATORI ESTERNI

Nel corso del 2010, in attuazione della decisione di procedere allo scorrimento della graduatoria di merito del concorso pubblico per funzionario con profilo giuridico-amministrativo, sono state immesse in servizio ulteriori 6 unità, che sono andate ad

aggiungersi a quelle già assunte nel corso del 2009 a seguito dei concorsi pubblici, per diverse posizioni, banditi dall'Autorità. Tali assunzioni hanno in parte coperto il fisiologico *turnover* di personale.

Inoltre, a conclusione della procedura selettiva per reclutare (sino) a 3 giovani laureati con contratto di specializzazione a tempo determinato della durata di un anno, sono stati immessi in servizio i relativi vincitori.

In considerazione delle perduranti carenze di personale, agli inizi del 2010 è stata, altresì, indetta una procedura selettiva per reclutare 4 funzionari con profilo giuridico da assumere con contratto a tempo determinato (avviso pubblico in *G.U.* –4a serie speciale– 26 febbraio 2010, n. 16). Tale procedura, finalizzata alla copertura dei 20 posti ancora vacanti nel contingente di personale con contratto a tempo determinato, previsto dall'art. 156, comma 5, del Codice, è stata ultimata nel corso dell'anno e i vincitori sono stati assunti agli inizi del 2011.

Nel periodo considerato si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2010 l'Ufficio poteva contare su un organico, a diverso titolo, di 109 unità, di cui 102 in servizio, al quale va aggiunto un contingente di personale a contratto di 16 unità, alcune delle quali peraltro assunte per brevi periodi.

Dai suddetti dati si evidenzia che nell'anno considerato non si è verificato un incremento del personale in servizio rispetto a quello dell'anno precedente, al netto delle cessazioni per varie cause, a fronte dei significativi incrementi già segnalati nella Relazione 2009.

Nel periodo considerato, l'Autorità ha fatto un limitato ricorso ad incarichi di collaborazione per completare alcuni progetti specifici e si è avvalsa, altresì, di alcune convenzioni per lo svolgimento di attività di natura esecutiva (ad es., per l'attività di portineria e per compiti ausiliari), ovvero per esigenze connesse a problematiche amministrativo-contabili e all'archiviazione e classificazione dei documenti.

Presso l'Autorità continua ad operare 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.

22.4. IL SETTORE INFORMATICO E TECNOLOGICO

Sviluppo del sistema informativo e dei servizi ICT

Nel corso del 2010 il Dipartimento risorse tecnologiche ha continuato l'attività di consolidamento del sistema informativo, con la cura diretta della manutenzione e del funzionamento, anche tramite servizi offerti nell'ambito delle convenzioni a favore delle pp.aa. negoziate dalle centrali d'appalto pubbliche. In particolare, è stato avviato il servizio di assistenza agli utenti (*helpdesk*) e di monitoraggio dei sistemi, con l'adesione alla Convenzione CNIPA "SPC - Conduzione di sistemi" e con la realizzazione di un presidio tecnico in sede, in grado di garantire il primo intervento e l'*escalation* in caso di emersione di problemi di maggiore complessità sulle piattaforme *hardware/software* controllate.

È proseguita comunque, pur nelle difficoltà dovute ai tagli di bilancio, l'opera di ammodernamento e razionalizzazione dell'infrastruttura informatica. In particolare, si è potenziata la piattaforma di virtualizzazione *VMware*, tramite cui sono erogati quasi tutti i servizi basati su server *Windows* o *Linux*, oltre ai sistemi di *storage* accessibili con tecnologia *Fibre Channel* nell'ambito di una "*Storage Area Network*". Il consolidamento dei sistemi ha consentito di centralizzare le procedure di *backup/restore* dei dati, e ottenere una migliore efficienza nella loro gestione. Si è provveduto a virtualizzare diversi sistemi *server*, tra cui quelli con cui viene erogato il servizio di notificazione telematica, effettuando la migrazione di tutti i contenuti senza interruzione di servizio, per raggiungere un più elevato livello di sicurezza e disponibilità, oltre che di semplicità gestionale.

È stata ulteriormente ampliata la digitalizzazione dei servizi della Biblioteca, con la messa a disposizione sulla rete intranet di *database* bibliografici e riviste *online*; sempre in relazione alla Biblioteca, è stato adottato il sistema "*Sebina OpenLibrary*" (SOL).

Sono stati sviluppati i servizi a supporto dell'attività informativa e comunicativa dell'Autorità, potenziando il servizio di rassegna stampa interna e pervenendo a una maggiore efficienza nella sua elaborazione.

È stata consolidata la piattaforma di intranet *online* per l'Ufficio, basata sull'infrastruttura *Microsoft Sharepoint*, integrata con i sistemi applicativi.

Sono state distribuite agli utenti interni le carte multiservizi basate sulla CNS (Carta nazionale dei servizi), con funzionalità di firma digitale, di *strong authentication* integrata

con le procedure di *smart logon* nei sistemi di rete *Windows* e di *badge* per il rilevamento delle presenze.

Impegno per la sicurezza informatica dell'Ufficio

Anche nel 2010 nessun incidente informatico è occorso nel dominio dell'Ufficio, e in particolare nessun evento relativo alla sicurezza ha mai prodotto danni o disservizi. Nessun *virus* informatico è penetrato nella rete interna attraverso canali di rete, mentre i controlli sui trasferimenti da supporti hanno consentito di bloccare ogni contenuto nocivo rilevato. Non si sono mai verificate perdite di dati, e alle occasionali indisponibilità di *file* o documenti, frutto per lo più di cancellazioni accidentali, è sempre stato possibile porre rimedio con le ordinarie procedure di *backup* e *recovery* o con i servizi di assistenza. La disponibilità dei servizi gestiti in modalità *in house* si è confermata sugli stessi livelli dell'anno precedente, con fermi macchina inferiori complessivamente alle 24 ore nell'arco dell'anno (riferiti ai servizi *online* di notificazione telematica e al sistema di posta elettronica) e quindi con disponibilità superiore al 99,7%, adeguata al contesto operativo dell'Autorità; ulteriori miglioramenti, seppure ipotizzabili, potrebbero comportare uno svantaggioso rapporto tra costi e benefici anche in considerazione del fatto che le poche ore annue di *downtime* di alcuni servizi sono per lo più dovute a condizioni strutturali esterne (rete elettrica, collegamenti telematici).

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento ha fornito nell'anno 2010 supporto alle unità dell'area giuridica dell'Ufficio, formulando analisi tecniche per le fasi istruttorie dei procedimenti dell'Autorità, ed approfondendo, con note informative e rapporti, argomenti a contenuto informatico-tecnologico. 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 affrontati.

Telecomunicazioni e Internet

Tra i principali interventi svolti si evidenziano, nell'ambito delle telecomunicazioni e di Internet: l'analisi tecnica della documentazione prodotta da *Google* con riferimento alla raccolta di dati relativi alla presenza e alla geolocalizzazione delle reti *wireless* di utenti italiani, effettuata contestualmente alla raccolta di immagini per il servizio *Street View*; la relazione sul fenomeno dell'invio di e-mail di invito all'iscrizione da parte di *Facebook* a soggetti inclusi tra i contatti all'interno delle rubriche degli utenti della *social network*; i

pareri resi per le risposte alle richieste di *prior checking* avanzate all'Autorità da parte di tutti gli operatori telefonici fissi e mobili per l'utilizzo di dati aggregati di traffico ai fini di profilazione della propria clientela; i pareri resi sul fenomeno delle attivazioni indesiderate di servizi mobili; le analisi in merito alla pubblicazione di documenti sui siti della p.a., con particolare riferimento ai princìpi di accessibilità dei dati ed alla loro possibile de-contestualizzazione. Di rilievo inoltre l'approfondimento degli aspetti tecnici legati all'attuazione della Direttiva n. 136/2009 sulle comunicazioni elettroniche (uso dei *cookie* per finalità di pubblicità comportamentale, notifica delle violazioni di dati personali "*data breaches*"), svolto dal Dipartimento sia attraverso relazioni e rapporti interni, sia attraverso seminari rivolti a dirigenti e funzionari dell'Ufficio.

Settore pubblico

Nell'ambito della collaborazione relativa a provvedimenti riguardanti il settore pubblico, si evidenziano le seguenti principali attività: parere sullo schema di regolamento interno del Ministero dell'ambiente per l'uso di e-mail e Internet [doc. *web* n. 1706464]; attività istruttoria relativa agli enti di riscossione, nonché verifica dell'adempimento da parte di Equitalia S.p.A. in relazione al *provvedimento* 7 ottobre 2009 [doc. *web* n. 1664231]; proroga per INPS, AGEA, AVCP sull'utilizzo di *web service* prevista dal *provvedimento* 18 settembre 2008 sull'Anagrafe tributaria [doc. *web* n. 1549548]; verifiche sull'adempimento alle prescrizioni relative al sistema N-SIS impartite al Ministero dell'interno (v. Relazione 2009, p. 3); analisi e consulenza sulla stesura dei provvedimenti finalizzati alla messa in sicurezza dei dati trattati dalla Giustizia amministrativa - Consiglio di Stato e TAR Lazio (*Provv.* 23 settembre 2010 [doc. *web* n. 1753845]).

Inoltre costante collaborazione è stata offerta nelle risposte a quesiti e richieste di chiarimento a carattere tecnico, in particolare nella fase applicativa del provvedimento sugli amministratori di sistema.

Contributi all'attività ispettiva

Anche nel 2010, nonostante l'accresciuta mole di lavoro sul fronte della consulenza interna, il Dipartimento risorse tecnologiche ha fornito proficuo supporto alle principali ispezioni dell'Autorità, intervenendo nella realizzazione di accessi a banche dati, con l'analisi e lo studio dei materiali acquisiti, con la stesura di rapporti e la formulazione di misure e accorgimenti di natura tecnologica. Tra le attività più significative si segnalano quelle

relative alle verifiche ispettive sul sistema informativo della fiscalità, gestito dall'Agenzia delle entrate, che costituisce una delle più rilevanti banche dati di interesse nazionale, e quelle condotte nell'ambito di enti previdenziali; gli accertamenti ispettivi sugli istituti credito, verificando nello specifico la struttura degli archivi, le tipologie di informazioni trattate, le procedure riguardanti gli accessi ai sistemi e alle applicazioni, i sistemi di autenticazione, le abilitazioni e le autorizzazioni degli utenti, le applicazioni utilizzate, le misure di sicurezza; gli accertamenti sugli operatori telefonici, nell'ambito dell'elaborazione di un provvedimento generale sulla profilazione dei dati personali; le attività ispettive in materia di riscossione; le attività ispettive sulle principali società emettitrici di carte di credito.

Contributi all'attività internazionale

Il Dipartimento risorse tecnologiche ha partecipato all'attività internazionale dell'Autorità nell'ambito sia dei gruppi di esperti nominati dalla Commissione europea su temi specifici, sia delle attività istituzionali del *Working Party* Art. 29, con studio di documenti e produzione di rapporti. Si segnalano in particolare, con riferimento al WP 29, la partecipazione ai lavori del *Technology Subgroup*, che affronta le tematiche di attualità nell'area ICT in materia di protezione dei dati personali, e del sottogruppo *STORK*, avente come scopo l'individuazione di una piattaforma europea interoperabile di *ID-management*. Di rilievo è stato poi il contributo fornito alla redazione del *report* pubblicato dal Gruppo Art. 29 sull'azione di *enforcement* comunitaria, svolta dalle autorità nazionali nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico e fornitori di accesso a Internet, relativa al recepimento, da parte degli Stati membri, della Direttiva n. 24/2006/CE sulla *data retention*, con particolare riferimento alle categorie di dati memorizzati, ai tempi di conservazione e alle misure tecnico organizzative per la conservazione dei dati di traffico telefonico e telematico. Si segnala inoltre la produzione di rapporti e relazioni tecniche connesse alla revisione del quadro normativo *ePrivacy*, come modificato dalla Direttiva n. 136/2009/CE.

Rilevante è stata poi la partecipazione a gruppi di lavoro, seminari e convegni internazionali e alle attività di divulgazione e comunicazione dell'Autorità. In tale ambito il Dipartimento ha contribuito ai lavori per la *Schengen Evaluation of Italy* del comitato di valutazione della *Joint Supervisory Authority* (JSA) (gennaio 2010).

22.5. IL MONITORAGGIO DELL'EFFICACIA E DELL'EFFICIENZA E IL SUPPORTO AL CONTROLLO INTERNO

Nel corso dell'anno 2010 è proseguito, a cura della competente Unità raccolta dati, flussi informativi e supporto al controllo interno, il monitoraggio delle attività svolte dalle unità organizzative dell'area giuridica e dall'Ufficio relazioni con il pubblico.

Le rilevazioni attengono alla ricognizione dei flussi documentali in entrata e in uscita, suddivisi per singole unità organizzative, raffrontati con le risorse umane.

Per fornire un monitoraggio costante, sia nel breve che nel lungo periodo, le rilevazioni sono molteplici ed hanno cadenza mensile, trimestrale, semestrale ed annuale; in particolare sono stati evidenziati i settori con maggiore quantità di affari da trattare, in maniera da fornire un indicatore sui profili di maggiore rilevanza e su eventuali criticità.

I *report* prodotti sono corredati da grafici e note esplicative che agevolano la percezione dei fenomeni evidenziati nelle tabelle.

Nel periodo di riferimento si è altresì provveduto ad incrementare il livello di analisi dei dati e dei *report*, nonché ad individuare ulteriori indicatori e parametri relativi alla gestione dell'attività principale dell'Ufficio.

È stata condotta inoltre una rilevazione straordinaria relativa alla ricognizione dei fascicoli arretrati in attesa di essere definiti; tale rilevazione ha consentito, tra l'altro, di individuare alcune cause sulla formazione dell'arretrato, nonché di prospettare possibili soluzioni per una ulteriore riduzione dello stesso.

È proseguita quindi l'attività di elaborazione di indicatori di efficienza-efficacia, relativi al rapporto tra pratiche definite ed effettive risorse disponibili.

Infine è stato istituito un gruppo di lavoro indirizzato all'esame di numerose problematiche emergenti dall'attuale sistema di protocollazione, con l'obiettivo di valutare l'eventuale sostituzione del prodotto attualmente in uso, anche al fine di implementare ulteriori funzionalità, quali lo sportello del cittadino o sistemi di *workflow* relativi ai procedimenti amministrativi in essere presso l'Ufficio.

PAGINA BIANCA

23. Dati statistici (*)

1. Sintesi delle principali attività dell'Autorità

SINTESI DELLE PRINCIPALI ATTIVITÀ DELL'AUTORITÀ	
Numero complessivo dei provvedimenti collegiali adottati	558
Ricorsi decisi (art. 145 del Codice)	349
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154 del Codice)	16
Altri provvedimenti collegiali	193
Notificazioni pervenute nell'anno 2010	1.197
Notificazioni pervenute dal 2004 al 31 dicembre 2010	18.756
Violazioni amministrative contestate	424
Sanzioni applicate con ordinanza di ingiunzione	98
Violazioni penali segnalate all'autorità giudiziaria	55
Riscontri a segnalazioni e reclami	3.698
Risposte a quesiti	387
Ricorsi (trattati) *ex* art. 152 del Codice	135
Opposizioni (trattate) a provvedimenti del Garante	65
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	474
Altre richieste ai sensi dell'art. 157 del Codice non effetuate direttamente presso i titolari	113
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	22
Provvedimenti su verifiche preliminari per trattamenti che presentano rischi specifici	7
Comunicazioni al Garante su flussi di dati tra p.a. o in temi di ricerca	10
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	4
Risposte ad atti di sindacato ispettivo e di controllo	4
Leggi regionali esaminate	20
(di cui con rilievi ai fini dell'impugnazione *ex* art. 127 della Costituzione)	(3)
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	23
Riunioni autorità comuni di controllo (Europol, Schengen, Dogane, Eurodac) e del *Wppj - Working Party on Police and Justice*	21
Riunioni presso organismi internazionali e *workshop*	15

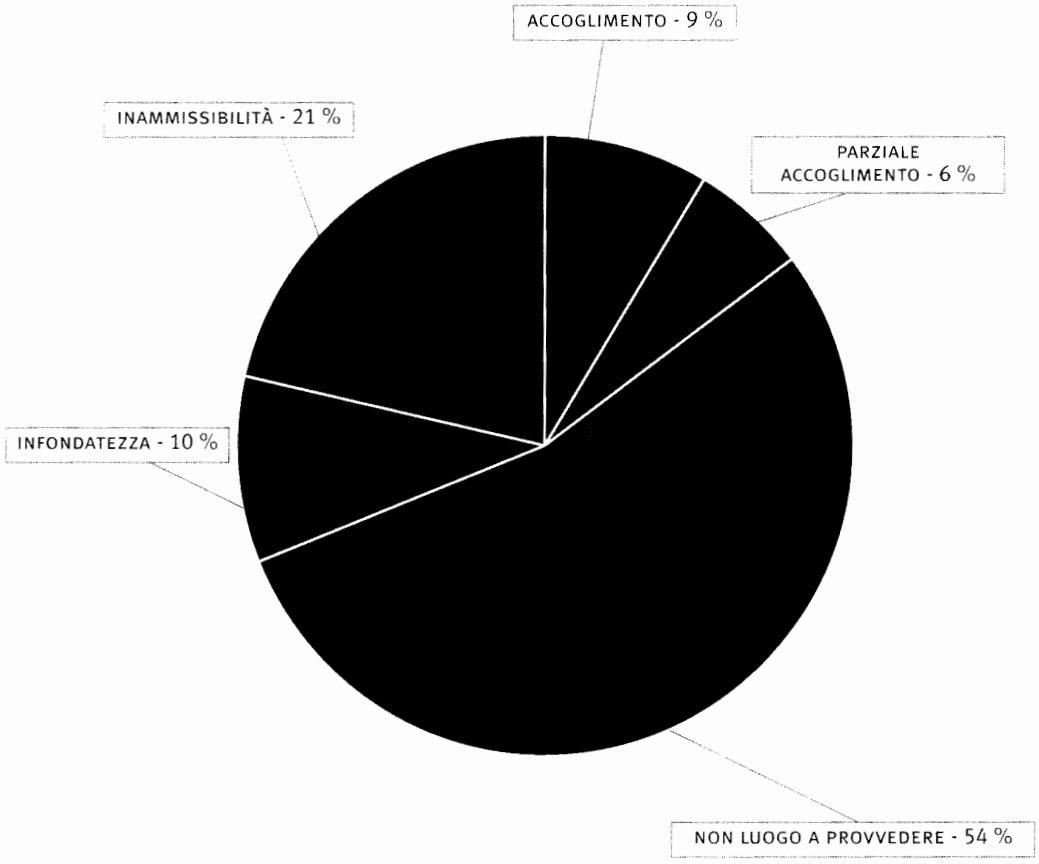
2. Altre attività

ALTRE ATTIVITÀ DELL'AUTORITÀ	
Comunicati stampa	27
Newsletter	12
Cd-rom (edizioni pubblicate)	1
Dépliant	2
Conferenze internazionali	4

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2010. Singole note indicano altri periodi o situazioni e casi specifici. I dati delle tabelle 8, 9, 10 si riferiscono ai fascicoli istituiti presso l'Ufficio

3. Tipologia delle decisioni su ricorsi (tabella e grafico)

DECISIONI SU RICORSI	
TIPI DI DECISIONE (1)	NUMERO RICORSI
Accoglimento	30
Parziale accoglimento	21
Non luogo a provvedere (2)	189
Infondatezza	34
Inammissibilità	75
Totale	**349**

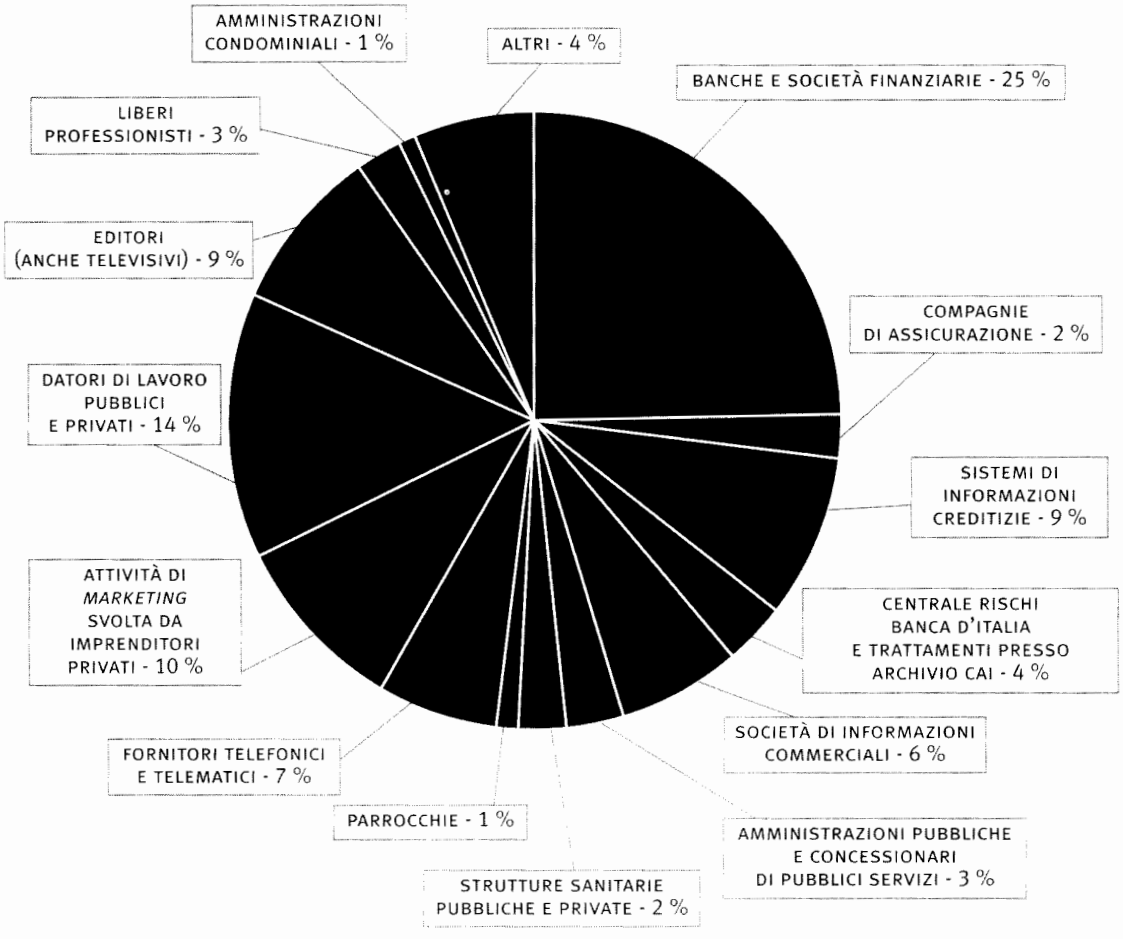


(1) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole"

(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)

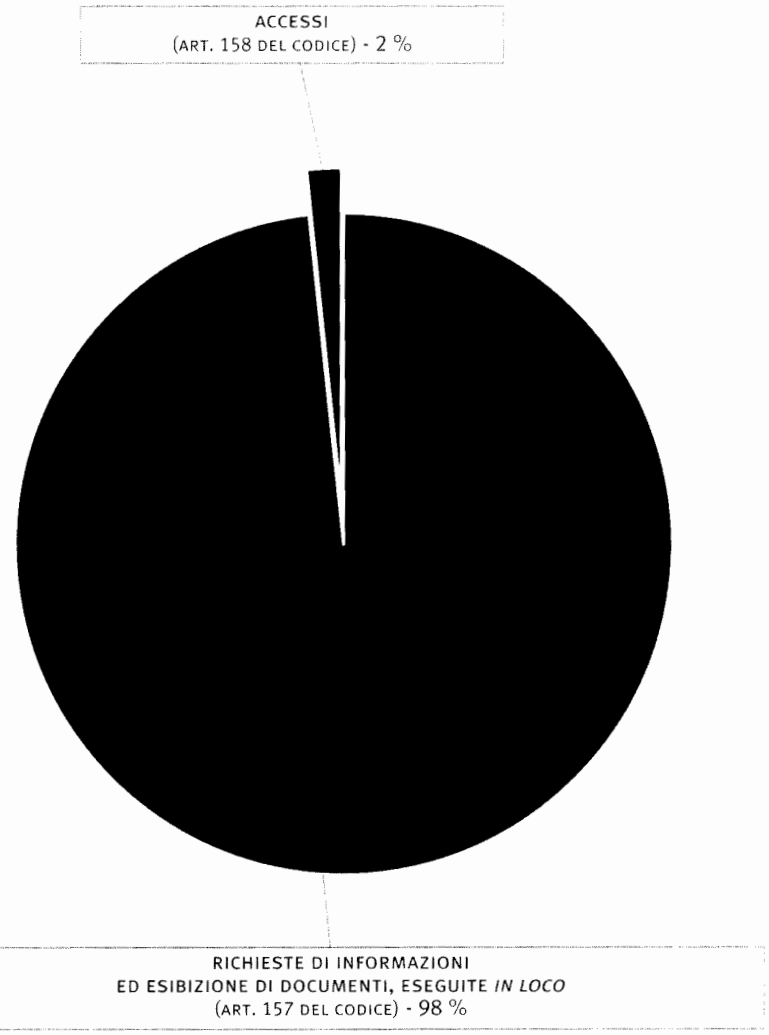
CATEGORIA DI TITOLARI	NUMERO RICORSI
Banche e società finanziarie	86
Compagnie di assicurazione	8
Sistemi di informazioni creditizie	30
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	12
Società di informazioni commerciali	22
Amministrazioni pubbliche e concessionari di pubblici servizi	11
Strutture sanitarie pubbliche e private	8
Parrocchie	4
Fornitori telefonici e telematici	23
Attività di *marketing* svolta da imprenditori privati	33
Datori di lavoro pubblici e privati	48
Editori (anche televisivi)	30
Liberi professionisti	9
Amministrazioni condominiali	3
Altri	22
Totale	**349**



5. Accertamenti e controlli eseguiti (tabella e grafico)

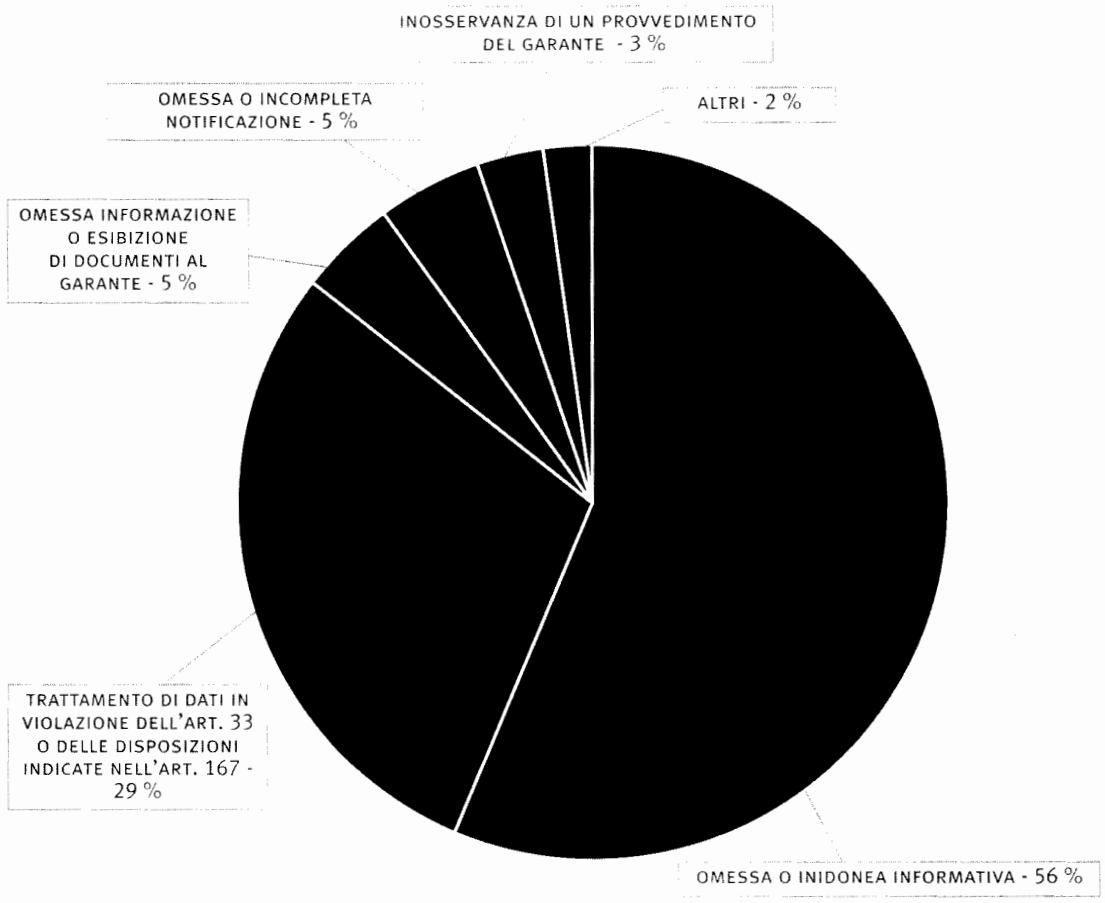
ACCERTAMENTI E CONTROLLI ESEGUITI DIRETTAMENTE PRESSO TITOLARI DEL TRATTAMENTO

TIPOLOGIA	NUMERO
Richieste di informazioni ed esibizione di documenti, eseguite *in loco* (art. 157 del Codice)	466
Accessi (art. 158 del Codice)	8
Totale	474



6. Violazioni amministrative contestate (tabella e grafico)

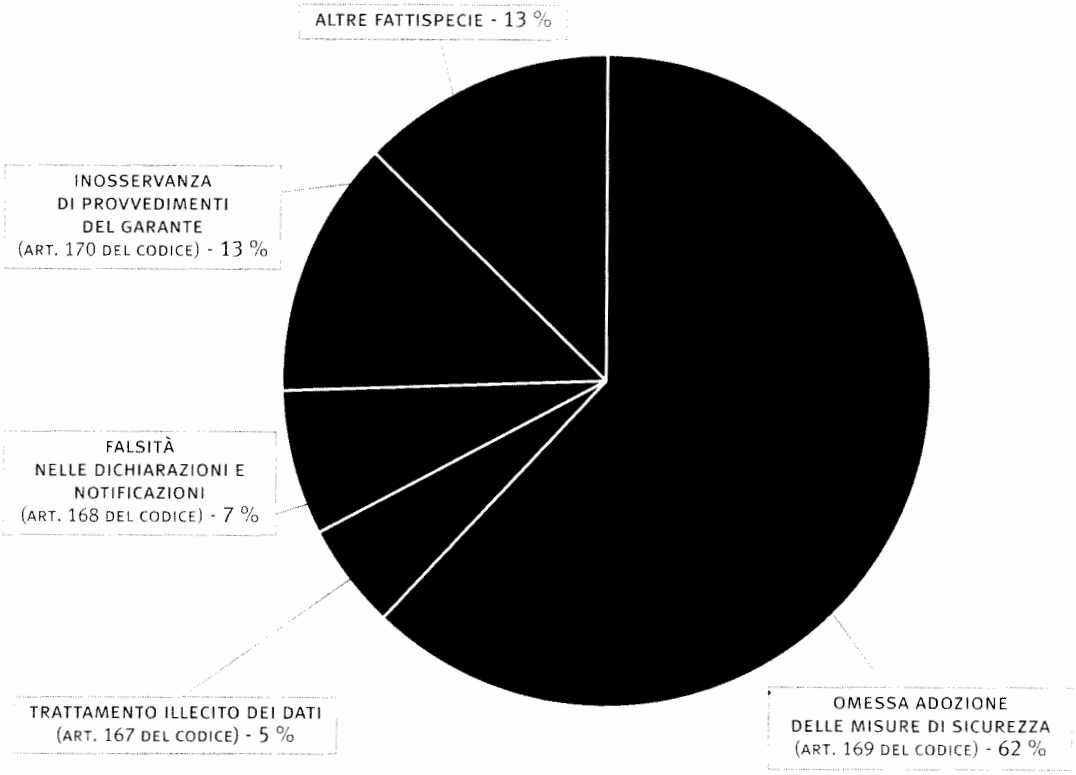
VIOLAZIONI AMMINISTRATIVE CONTESTATE		
Omessa o inidonea informativa (art. 161 del Codice)		239
Trattamento di dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)		124
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)		19
Omessa o incompleta notificazione (art. 163 del Codice)		20
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)		12
Sanzioni in materia di conservazione di dati di traffico (art. 162-*bis* del Codice)(1)		4
Più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice) (1)		6
	Totale	424
Somme versate a titolo di oblazione in via breve		3.046.001
Somme versate in conseguenza di ordinanze di ingiunzione		306.400
	Totale	**3.352.401**



(1) Valore indicato nel grafico sotto la voce "altri"

7. Violazioni penali segnalate all'autorità giudiziaria (tabella e grafico)

VIOLAZIONI PENALI SEGNALATE ALL'AUTORITÀ GIUDIZIARIA	SEGNALAZIONI
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	34
Trattamento illecito dei dati (art. 167 del Codice)	3
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	4
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	7
Altre fattispecie	7
Totale	55
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	457.500



8. Pareri (art. 154, comma 4, del Codice)

PARERI (ART. 154, COMMA 4, DEL CODICE) TEMI	RISCONTRI RESI NELL'ANNO (1)
Attività di polizia, sicurezza nazionale e governo del territorio	3
Giustizia	1
Informatizzazione e banche dati della p.a.	5
Formazione	2
Rapporto di lavoro pubblico	1
Tutela della salute e attività sanitaria	1
Soggetti privati e attività produttive	1
Solidarietà sociale	1
Marketing telefonico	1
Totale	16

(1) Inerenti anche ad affari pervenuti anteriormente al 2010

9. Quesiti

QUESITI	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	**353**	**387**
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	17	18
Dati dei dipendenti e fascicoli personali	12	16
Giornalismo	2	3
Giustizia e accertamenti di polizia	5	5
Internet e informatizzazione	7	13
Rilevazioni biometriche	4	7
Sanità e servizi di assistenza sociale	13	30
Telefonia	6	6
Trasparenza	13	11
Tributi	3	10
Videosorveglianza	27	26

10. Segnalazioni e reclami

SEGNALAZIONI E RECLAMI	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	**3.359**	**3.698**
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	15	9
Assicurazioni	118	110
Associazioni	35	23
Centrali rischi	250	213
Concessionari pubblici servizi	161	134
Condominio	29	29
Corrispondenza	8	15
Credito	197	187
Dati dei dipendenti e fascicoli personali	45	57
Giornalismo	52	97
Giustizia e accertamenti di polizia	27	45
Imprese	121	73
Informazioni commerciali	14	3
Internet e informatizzazione	77	140
Lavoro	122	89
Marketing	48	82
Pubblicità non gradita	33	49
Recupero crediti	128	128
Rilevazioni biometriche	10	12
Sanità e servizi di assistenza sociale	32	49
Telefonia	279	479
Trasparenza	10	17
Tributi	11	49
Videosorveglianza	211	139

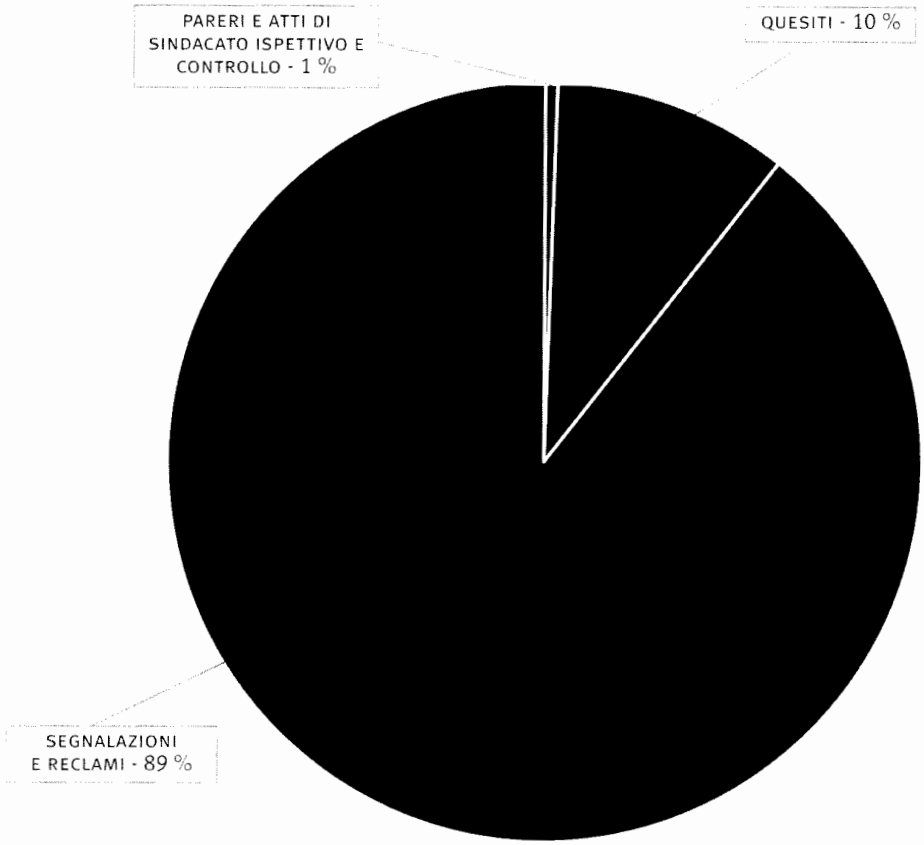
(1) Inerenti anche ad affari pervenuti anteriormente al 2010

11. Atti di sindacato ispettivo e controllo

ATTI DI SINDACATO ISPETTIVO E CONTROLLO

TEMI	NUMERO
Sms di propaganda elettorale	1
Requisiti per il possesso di porto d'armi	1
Trattamento dei dati di utenze di cellulari	1
Tutela del diritto d'autore in relazione a condotte realizzate attraverso siti *peer to peer*	1
Totale	4

12. Tipologie dei riscontri resi a interessati e richiedenti



13. Tipologie di notificazioni pervenute nel 2010

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL 2010 (1)

	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)	TOTALE EURO
Prima notificazione al Garante	42	694	736	
Modifica di una precedente notificazione	15	370	385	
Notificazione della cessazione del trattamento	14	62	76	
Totale	71	1.126	1.197	179.550

(1) I valori sono riferiti alla data del 31 dicembre 2010

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL PERIODO 2004-2010

	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	1.095	14.751	15.846
Modifica di una precedente notificazione	86	2.305	2.391
Notificazione della cessazione del trattamento	54	465	519
Totale	**1.235**	**17.521**	**18.756**

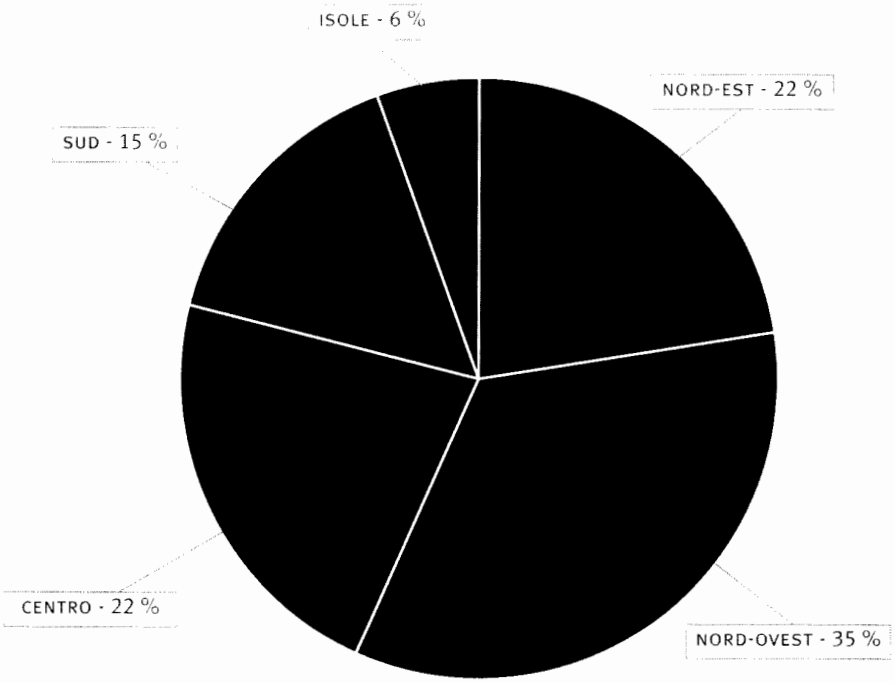
14. Tipologie di notificazioni pervenute nel periodo 2004-2010

PROVENIENZA GEOGRAFICA DELLE NOTIFICAZIONI NEL PERIODO 2004-2010

ITALIA

ZONE GEOGRAFICHE	PERVENUTE
Nord-Est	4.201
Nord-Ovest	6.394
Centro	4.164
Sud	2.868
Isole	1.051
Totale	**18.678**
Da altri Paesi	78

15. Provenienza geografica delle notificazioni nel periodo 2004-2010 (tabella e grafico)

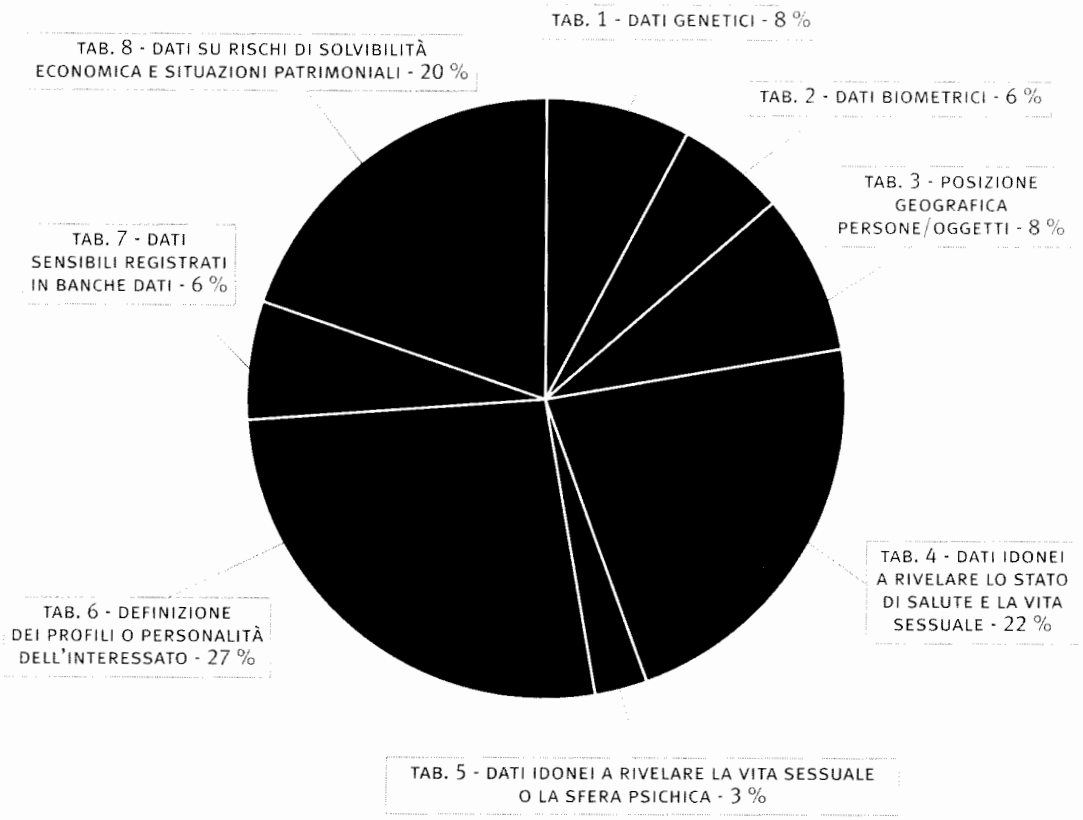


(1) Situazione alla data del 31 dicembre 2010

16. Suddivisione delle notificazioni per tipologia di trattamento periodo 2004-2010 (tabella e grafico)

SUDDIVISIONE DELLE NOTIFICAZIONI PER TIPOLOGIA DI TRATTAMENTO PERIODO 2004-2010

TABELLE DI NOTIFICAZIONE COMPILATE (1)	NUMERO
Tabella 1 - Trattamento di dati genetici	2.180
Tabella 2 - Trattamento di dati biometrici	1.584
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	2.348
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, 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	6.206
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica ad opera di associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	749
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	7.372
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	1.769
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	5.468
Totale	**27.676**



(1) Situazione alla data del 31 dicembre 2010

MODALITÀ DI INOLTRO DELLE NOTIFICAZIONI PERIODO 2004-2010

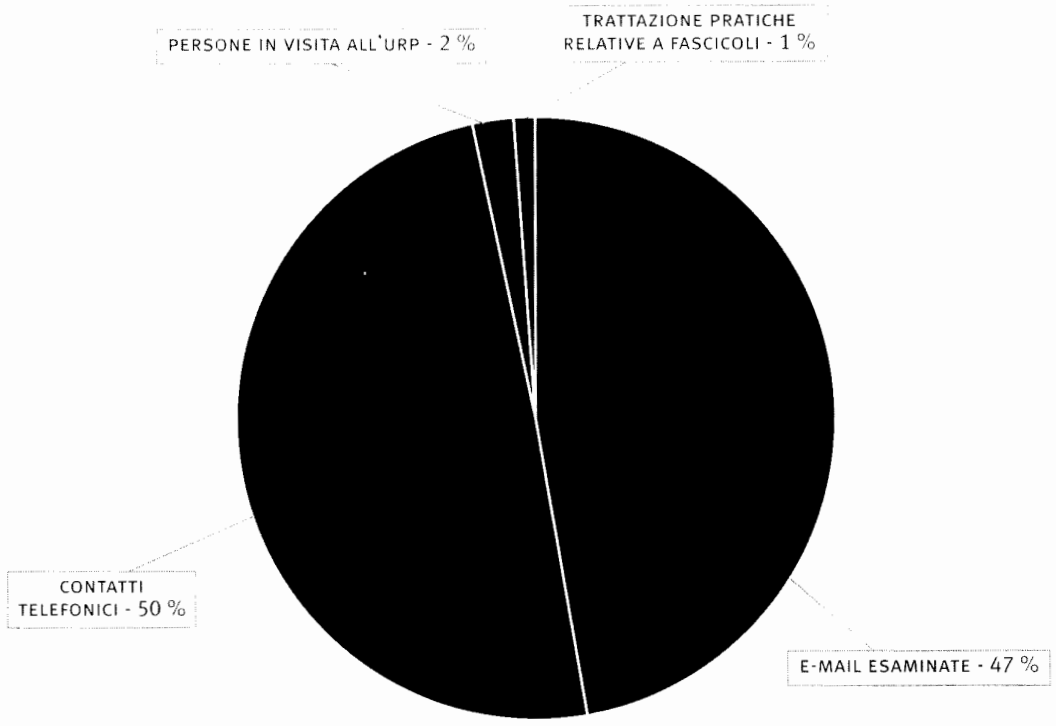
Attraverso intermediari		9.544
Direttamente a cura dei titolari		9.212
	Totale	**18.756**

17. Modalità di inoltro delle notificazioni periodo 2004-2010

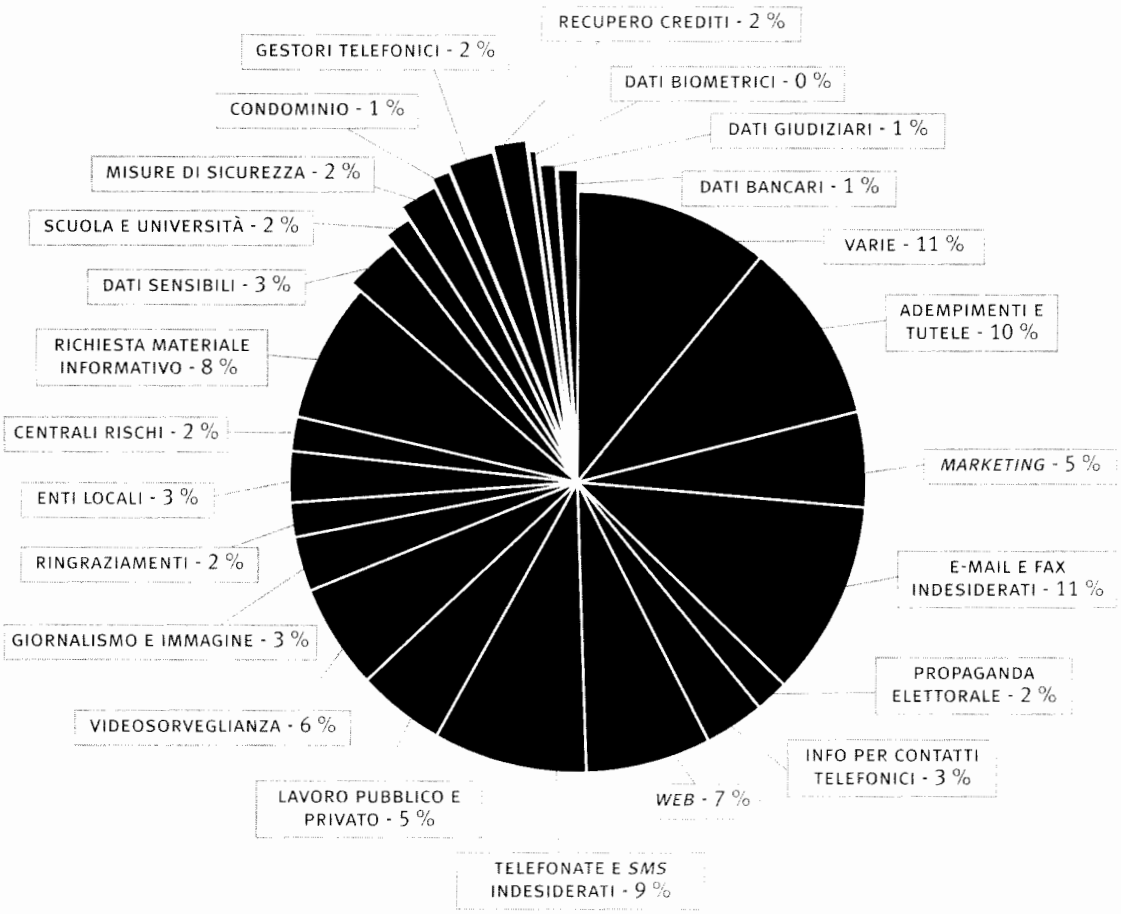
UFFICIO RELAZIONI CON IL PUBBLICO

	2010
E-mail esaminate	12.610
Contatti telefonici	12.767
Persone in visita all'URP	571
Trattazione pratiche relative a fascicoli	295
Totale	**26.243**

18. Ufficio relazioni con il pubblico (tabella e grafico)



19. E-mail esaminate dall'Ufficio relazioni con il pubblico [grafico delle categorie]



20. 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

21. 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	15	3	4	14
Funzionari	59	5	3	61
Operativi	24	2		26
Esecutivi				0
Totale	**99**	**10**	**7**	**102**
Personale a contratto				16

22. Risorse finanziarie

RISORSE FINANZIARIE

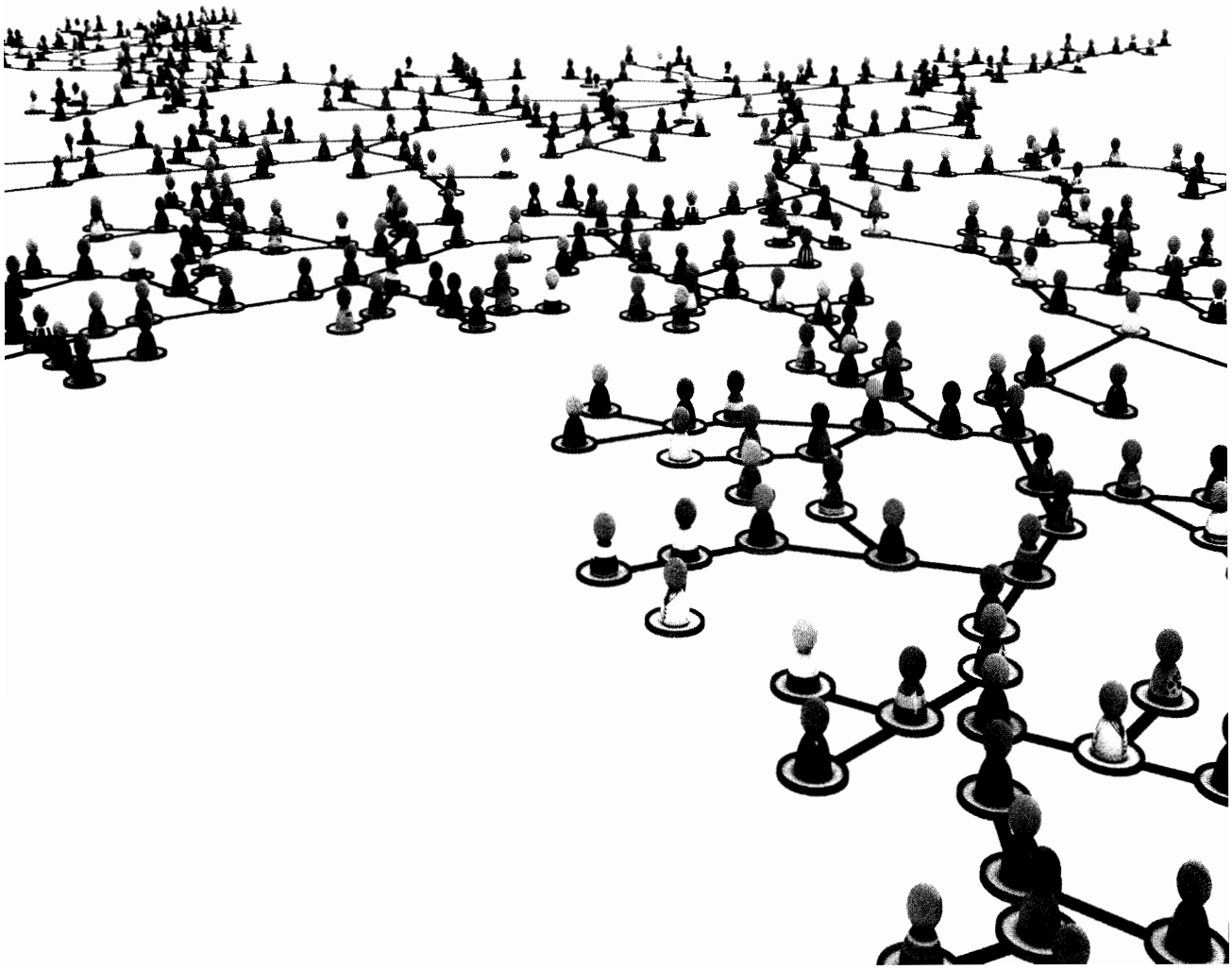
ENTRATE ACCERTATE	ANNO 2010	ANNO 2009	DIFFERENZA
Correnti	16.606.197	15.317.835	1.288.362
di cui trasferimento dallo Stato	13.373.059	13.135.167	237.892
Totale entrate	**16.606.197**	**15.317.835**	**1.288.362**

SPESE IMPEGNATE	ANNO 2010	ANNO 2009	DIFFERENZA
Funzionamento	17.616.735	24.124.022	- 6.507.287
Capitale	114.742	438.755	- 324.013
Totale spese	**17.731.477**	**24.562.777**	**- 6.831.300**

(1) Situazione alla data del 31 dicembre 2010

PAGINA BIANCA

Documentazione



PAGINA BIANCA

IV. Documentazione

24. Provvedimenti del Garante

Posta elettronica aziendale e *privacy* del dipendente

21 gennaio 2010 [doc. *web* n. 1701577]

Pubblicità degli incarichi conferiti dalle amministrazioni pubbliche

21 gennaio 2010 [doc. *web* n. 1694419]

Assorbimento della tessera sanitaria (TS) nella carta nazionale dei servizi (CNS)

21 gennaio 2010 [doc. *web* n. 1693904]

Sistema di informazione visti (VIS) e scambio di dati fra gli Stati membri dell'Unione europea

28 gennaio 2010 [doc. *web* n. 1694785]

Misure in materia di propaganda elettorale - esonero dall'informativa

11 febbraio 2010 [doc. *web* n. 1694531]

Riservatezza dei dati bancari

11 febbraio 2010 [doc. *web* n.1705119]

18 marzo 2010 [doc. *web* n. 1715015]

Trattamento di dati personali del dipendente mediante sistemi di localizzazione satellitare

18 febbraio 2010 [doc. *web* n. 1703103]

Richiesta di cancellazione dei dati personali dall'archivio *online* di un quotidiano

18 febbraio 2010 [doc. *web* n. 1706475]

Censimento generale dell'agricoltura: trattamento di dati personali e tutela della riservatezza
18 febbraio 2010 [doc. *web* n. 1703119]

Richiesta di cancellazione *online* della cd. "etichetta" (*tag*) in un profilo *Facebook*
18 febbraio 2010 [doc. *web* n. 1712776]

In bagno senza il permesso dell'azienda
24 febbraio 2010 [doc. *web* n. 1705070]

Trattamento di dati personali nei servizi di assistenza telefonica
4 marzo 2010 [doc. *web* n. 1721214]

Utilizzo della posta elettronica e della rete Internet presso il Ministero dell'ambiente
4 marzo 2010 [doc. *web* n. 1706464]

Preiscrizioni universitarie per l'anno accademico 2010/2011
4 marzo 2010 [doc. *web* n. 1706122]

Pubblico registro automobilistico e *privacy*
11 marzo 2010 [doc. *web* n. 1709295]

Trattamento di informazioni sulla solvibilità e affidabilità dei clienti da parte di una banca
11 marzo 2010 [doc. *web* n. 1715024]

Accessi all'anagrafe tributaria tramite *web service*: proroga degli adempimenti e sicurezza
26 marzo 2010 [doc. *web* n. 1713453]
21 ottobre 2010 [doc. *web* n. 1767204]
2 dicembre 2010 [doc. *web* n. 1776140]
9 dicembre 2010 [doc. *web* n. 1780265]

Esonero dall'informativa per un sito *web* che raccoglie e diffonde dati già disponibili *online*

26 marzo 2010 [doc. *web* n. 1721169]

Marketing: necessario il consenso per l'invio di comunicazioni promozionali via e-mail

26 marzo 2010 [doc. *web* n. 1727662]

8 aprile 2010 [doc. *web* n. 1721205]

23 settembre 2010 [doc. *web* n. 1758527]

Marketing via fax: necessario il consenso preventivo dell'interessato

26 marzo 2010 [doc. *web* n. 1719901]

26 marzo 2010 [doc. *web* n. 1719891]

Ricerche di tipo sociologico su aderenti a confessioni religiose: profili attinenti alla protezione dei dati

1° aprile 2010 [doc. *web* n. 1721183]

Controlli sull'utilizzo della rete Internet da parte del lavoratore

1° aprile 2010 [doc. *web* n. 1717799]

Trattamento dei dati sensibili e giudiziari presso la Commissione nazionale per le società e la borsa

8 aprile 2010 [doc. *web* n. 1718426]

Autorizzazione al trasferimento di dati personali verso Paesi non appartenenti all'UE mediante *BCR*

8 aprile 2010 [doc. *web* n. 1717863]

7 ottobre 2010 [doc. *web* n. 1763052]

Provvedimento in materia di videosorveglianza

8 aprile 2010 [doc. *web* n. 1712680]

No alla ricerca in tv degli adottati

8 aprile 2010 [doc. *web* n. 1718160]

6 maggio 2010 [doc. *web* n. 1718239]

Posta elettronica aziendale e *privacy* del dipendente

22 aprile 2010 [doc. *web* n. 1727692]

Accesso dell'interessato a dati personali riguardanti la gestione del rapporto di lavoro

22 aprile 2010 [doc. *web* n. 1724445]

Autorizzazione per uno studio epidemiologico senza consenso informato

27 aprile 2010 [doc. *web* n. 1722683]

16 settembre 2010 [doc. *web* n. 1753153]

4 novembre 2010 [doc. *web* n. 1767796]

Richiesta di cancellazione di dati inerenti ad una situazione debitoria

27 aprile 2010 [doc. *web* n. 1733190]

22 luglio 2010 [doc. *web* n. 1748844]

Trattamento di dati personali in occasione di richieste di finanziamento

6 maggio 2010 [doc. *web* n. 1737818]

Fax e mail promozionali: illeciti senza consenso

6 maggio 2010 [doc. *web* n. 1729175]

13 maggio 2010 [doc. *web* n. 1737799]

3 giugno 2010 [doc. *web* n. 1738039]

1° luglio 2010 [doc. *web* n. 1738592]

10 novembre 2010 [doc. *web* n. 1769487]

Prove di ammissione ai corsi di laurea ad accesso programmato per l'anno accademico 2010/2011

6 maggio 2010 [doc. *web* n. 1722452]

Scuola: vietata la comunicazione di dati personali relativi agli allievi minorenni

13 maggio 2010 [doc. *web* n. 1738356]

Disabili al supermercato: solo dati essenziali

13 maggio 2010 [doc. *web* n. 1729156]

Richiesta di cancellazione di dati personali da siti Internet

13 maggio 2010 [doc. *web* n. 1735420]

Registro pubblico delle opposizioni e tutela della riservatezza

13 maggio 2010 [doc. *web* n. 1734800]

Privacy e agenzie di *rating*: maggiori controlli sui conflitti di interesse

19 maggio 2010 [doc. *web* n. 1736161]

Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE

27 maggio 2010 [doc. *web* n. 1728496]

Tutela della riservatezza in caso di infezioni da *HIV*

27 maggio 2010 [doc. *web* n. 1738383]

Rigetto di istanze di autorizzazione formulate in ordine al trattamento dei dati giudiziari previsti dal *Sarbanes - Oxley Act* (e dalla relativa disciplina di attuazione)

3 giugno 2010 [doc. *web* n. 1737838]

3 giugno 2010 [doc. *web* n. 1737844]

3 giugno 2010 [doc. *web* n. 1737997]

3 giugno 2010 [doc. *web* n. 1738015]

3 giugno 2010 [doc. *web* n. 1738024]

3 giugno 2010 [doc. *web* n. 1738030]

3 giugno 2010 [doc. *web* n. 1738053]

3 giugno 2010 [doc. *web* n. 1738372]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni

3 giugno 2010 [doc. *web* n. 1734459]

15 luglio 2010 [doc. *web* n. 1746654]

22 luglio 2010 [doc. *web* n. 1748818]

29 settembre 2010 [doc. *web* n. 1763552]

Trattamento di dati relativi alle manifestazioni a premio e tutela della riservatezza

3 giugno 2010 [doc. *web* n. 1734810]

Aggiornamento 2010 del Programma statistico nazionale 2008-2010

10 giugno 2010 [doc. *web* n. 1734415]

No alla *webcam* in negozio senza tutele per i lavoratori

10 giugno 2010 [doc. *web* n. 1736167]

Registro nazionale delle persone che non hanno fissa dimora

10 giugno 2010 [doc. *web* n. 1741747]

Controlli sull'utilizzo del *personal computer* aziendale da parte del lavoratore

10 giugno 2010 [doc. *web* n. 1736780]

Autonoleggio e garanzie nel trattamento dati personali

16 giugno 2010 [doc. *web* n. 1741982]

Trattamento di dati personali nell'ambito della Anagrafe nazionale degli studenti

16 giugno 2010 [doc. *web* n. 1734404]

Tessera del tifoso e protezione dei dati personali

16 giugno 2010 [doc. *web* n. 1733656]

Prescrizioni per la videosorveglianza in un centro per la riabilitazione

24 giugno 2010 [doc. *web* n. 1738396]

Modifiche ed integrazioni al codice dell'amministrazione digitale

24 giugno 2010 [doc. *web* n. 1737729]

Trattamento di dati relativi a donne che lasciano il lavoro per maternità

1° luglio 2010 [doc. *web* n. 1737773]

Articoli pubblicati sul *web*: vietata la diffusione di dati sensibili

1° luglio 2010 [doc. *web* n. 1738303]

Richiesta di cancellazione di un articolo pubblicato *online* contenente dati personali

1° luglio 2010 [doc. *web* n. 1746519]

Bacheche condominiali: gli avvisi non devono contenere dati personali

8 luglio 2010 [doc. *web* n. 1741950]

Raccolta di dati via Internet per finalità promozionali: sempre necessario il consenso degli interessati

15 luglio 2010 [doc. *web* n. 1741998]

Regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione

15 luglio 2010 [doc. *web* n. 1741725]

Nella banca dati sulla pedofilia massima riservatezza per le vittime

22 luglio 2010 [doc. *web* n. 1741941]

Comunicazione di dati sui passeggeri che entrano in Italia da parte dei vettori aerei

22 luglio 2010 [doc. *web* n. 1741930]

Concorsi *online* e *web* radio: no alla profilazione occulta

22 luglio 2010 [doc. *web* n. 1741988]

Assemblee di condominio: vietate ai soggetti esterni non legittimati

9 settembre 2010 [doc. *web* n. 1758751]

Comunicazioni "captate" su reti *Wi-Fi*: il Garante ordina a *Google Street View* il blocco dei dati e trasmette gli atti alla magistratura

9 settembre 2010 [doc. *web* n. 1750529]

In tv più tutele per i minori vittime di violenza

16 settembre 2010 [doc. *web* n. 1753383]

Centrali rischi e garanzie per i consumatori

16 settembre 2010 [doc. *web* n. 1753816]

Rigetto dell'istanza di autorizzazione riguardante l'esonero dell'informativa da rendere agli interessati con riguardo al trattamento di dati presenti nel *database* telefonico unico (DBU)

16 settembre 2010 [doc. *web* n. 1753351]

Programma statistico nazionale 2011-2013

23 settembre 2010 [doc. *web* n. 1753181]

Giustizia amministrativa più protetta

23 settembre 2010 [doc. *web*. n. 1753845]

Trattamento di dati giudiziari del dipendente in una causa di licenziamento

23 settembre 2010 [doc. *web* n. 1756065]

Regione Liguria: elaborazioni statistiche nell'ambito della procedura sperimentale per l'acquisizione dei dati di mortalità

23 settembre 2010 [doc. *web* n. 1753195]

Ricorso al Garante: interpello preventivo e inammissibilità

23 settembre 2010 [doc. *web* n. 1761903]

21 ottobre 2010 [doc. *web* n. 1768206]

Ordinanze di custodia cautelare *online*: sì, ma solo con dati essenziali

29 settembre 2010 [doc. *web* n. 1763096]

Accesso dell'interessato a dati contenuti nel fascicolo personale attinente la procedura di licenziamento

29 settembre 2010 [doc. *web* n. 1765061]

Attività di profilazione dei clienti, invio di comunicazioni promozionali e cessione di dati a terzi per finalità commerciali: è necessario il consenso degli interessati

7 ottobre 2010 [doc. *web* n. 1763037]

Bloccata la localizzazione dei dipendenti di un'azienda

7 ottobre 2010 [doc. *web* n. 1763071]

Google Street View: le auto dovranno essere riconoscibili

15 ottobre 2010 [doc. *web* n. 1759972]

Comunicazione di informazioni eccedenti e non pertinenti in ambito bancario

21 ottobre 2010 [doc. *web* n. 1771017]

Istanze di congedo ordinario: i dipendenti non sono tenuti a produrre documenti per giustificare le richieste

4 novembre 2010 [doc. *web* n. 1779735]

Verifica preliminare: conservazione di immagini per un periodo eccedente i tempi fissati dal provvedimento generale del Garante in materia di videosorveglianza

4 novembre 2010 [doc. *web* n. 1767759]

Verifica preliminare: trattamento di dati personali connesso ad un sistema di valutazione dei dipendenti

4 novembre 2010 [doc. *web* n. 1771838]

Trattamento di dati sensibili riferiti ad una terza persona in una causa di separazione

4 novembre 2010 [doc. *web* n. 1770943]

Servizi finanziari e informativa ai clienti

10 novembre 2010 [doc. *web* n. 1769502]

Tessera del tifoso: più garanzie per i *supporter*

10 novembre 2010 [doc. *web* n. 1779725]

Trasporto: impronte digitali solo in casi particolari

17 novembre 2010 [doc. *web* n. 1779745]

17 novembre 2010 [doc. *web* n. 1779758]

Contraccezione e minori: no all'accesso dei genitori alle prescrizioni

17 novembre 2010 [doc. *web* n. 1769451]

Accesso dell'interessato a dati contenuti nel fascicolo personale e differimento per far valere un diritto in giudizio

17 novembre 2010 [doc. *web* n. 1778268]

Regolamento di attuazione della legge 22 dicembre 1999, n. 512, concernente il Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso

17 novembre 2010 [doc. *web* n. 1779672]

Violazione della *privacy* nell'ambito dei processi: l'ultima parola al giudice

17 novembre 2010 [doc. *web* n. 1779765]

Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica
2 dicembre 2010 [doc. *web* n. 1774813]

Modalità tecniche relative alla trasmissione da parte dei comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero
2 dicembre 2010 [doc. *web* n. 1779678]

Assicurazioni auto: trattamento di dati personali nell'ambito di servizi di preventivazione tramite *call center*
2 dicembre 2010 [doc. *web* n. 1780277]

Postel: esonero dall'informativa per il trattamento di dati personali a fini di *marketing* postale
16 dicembre 2010 [doc. *web* n. 1781973]

Delibera CICR relativa all'accesso dei finanziatori degli Stati membri dell'Unione europea ai sistemi informazione creditizia
16 dicembre 2010 [doc. *web* n. 1779694]

Trattamento di dati personali da parte di un'associazione politica
23 dicembre 2010 [doc. *web* n. 1784951]

Ulteriore differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici, rilasciata il 22 febbraio 2007
23 dicembre 2010 [doc. *web* n. 1776159]

Trattamento dei dati sensibili e giudiziari effettuati dalla Banca d'Italia e dall'Ufficio italiano dei cambi
13 gennaio 2011 [doc. *web* n. 1787870]

Controlli sull' utilizzo del telefono cellulare aziendale in dotazione ad un dipendente
13 gennaio 2011 [doc. *web* n. 1792605]

Giornalismo: essenzialità dell'informazione e diffusione di dati clinici
13 gennaio 2011 [doc. *web* n. 1787902]

Prenotazioni e ritiro analisi in farmacia: via libera del Garante *Privacy*
19 gennaio 2011 [doc. *web* n. 1787887]

Ricerca epidemiologica sui militari in Bosnia
19 gennaio 2011 [doc. *web* n. 1787877]

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
19 gennaio 2011 [doc. *web* n. 1784528]

Prescrizioni all'ISTAT sulle modalità di pubblicazione dell'informativa sul trattamento di dati personali nell'ambito del 15° censimento generale della popolazione e delle abitazioni
19 gennaio 2011 [doc. *web* n. 1784974]

Scambio di informazioni tra i Ministeri dell'interno e delle infrastrutture e dei trasporti ai fini del rilascio e della revoca dei titoli abilitativi alla guida di veicoli, motoveicoli e ciclomotori
26 gennaio 2011 [doc. *web* n. 1790365]

Trattamento di dati giudiziari riguardanti i candidati alle consultazioni elettorali regionali
3 febbraio 2011 [doc. *web* n. 1790414]

Trattamento di dati per attività giornalistica ed esercizio del diritto di cronaca
3 febbraio 2011 [doc. *web* n. 1793828]

Autorità per l'energia elettrica e il gas: trattamento di dati sensibili e giudiziari in relazione a finalità di rilevante interesse pubblico
3 febbraio 2011 [doc. *web* n. 1790422]

Modelli di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati ai servizi di telefonia fissa e mobile
24 febbraio 2011 [doc. *web* n. 1794638]

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*
2 marzo 2011 [doc. *web* n. 1793203]

25. PRINCIPALI ATTIVITÀ INTERNAZIONALI

25.1. UNIONE EUROPEA

REVISIONE DELLA DIRETTIVA N. 95/46/CE

Comunicazione (2010)609 della Commissione - Un approccio globale alla protezione dei dati personali nell'Unione europea

4 novembre 2010 [doc. *web* n. 1807279]

DIRITTI FONDAMENTALI

Comunicazione (2010)573 della Commissione - Strategia per un'attuazione effettiva della Carta dei diritti fondamentali dell'Unione europea

19 ottobre 2010 [doc. *web* n. 1807269]

SPAZIO EUROPEO DI LIBERTÀ, SICUREZZA E GIUSTIZIA

Comunicazione (2010)171 della Commissione - Piano d'azione per l'attuazione del programma di Stoccolma

24 aprile 2010 [doc. *web* n. 1807250]

ACCORDO UE-USA IN MATERIA DI DATI FINANZIARI

Risoluzione legislativa del Parlamento europeo sul progetto di decisione del Consiglio relativa all'accordo UE-USA sul trasferimento di dati di messaggistica finanziaria ai fini del programma di controllo delle transazioni finanziarie dei terroristi

8 luglio 2010 [doc. *web* n. 1810135]

Decisione del Consiglio sull'accordo UE-USA sul trasferimento di dati di messaggistica finanziaria per il programma di controllo delle transazioni finanziarie dei terroristi

13 luglio 2010 [doc. *web* n. 1807254]

Accordo UE-USA sul trasferimento di dati di messaggistica finanziaria ai fini del programma di controllo delle transazioni finanziarie dei terroristi

27 luglio 2010 [doc. *web* n. 1807980]

PROPRIETÀ INTELLETTUALE

Risoluzione 2009/2178(INI) del Parlamento europeo sull'applicazione dei diritti di proprietà intellettuale nel mercato interno

22 settembre 2010 [doc. *web* n. 1808032]

PUBBLICITÀ COMPORTAMENTALE

Risoluzione 2010/2052(INI) del Parlamento europeo sull'impatto della pubblicità sul comportamento del consumatore

15 dicembre 2010 [doc. *web* n. 1807285]

ADEGUATEZZA DI PAESI TERZI

Decisione 2010/625/UE della Commissione sull'adeguata protezione dei dati personali ad Andorra

19 ottobre 2010 [doc. *web* n. 1807275]

Decisione 2011/61/UE della Commissione sull'adeguata protezione dei dati personali da parte dello Stato d'Israele

31 gennaio 2011 [doc. *web* n. 1807299]

EURODAC

Controllo coordinato di EURODAC - Rapporto annuale 2008-2009

[doc. *web* n. 1807305]

25.2. CORTE DI GIUSTIZIA DELLE COMUNITÀ EUROPEE

INDIPENDENZA DELLE AUTORITÀ

Commissione contro Repubblica federale di Germania C-518/07

9 marzo 2010 [doc. *web* n. 1807323]

BILANCIAMENTO ACCESSO ATTI PUBBLICI E PROTEZIONE DATI

Commissione contro *Bavarian Lager Co. Ltd* C-28/08 P

29 giugno 2010 [doc. *web* n. 1807971]

25.3. GRUPPO ART. 29

WP 169 - Parere 1/2010 sui concetti di "*data controller*" e "*data processor*"

16 febbraio 2010 [doc. *web* n. 1791958]

WP 171 - Parere 2/2010 sulla pubblicità comportamentale *online*

22 giugno 2010 [doc. *web* n. 1791964]

WP 173 - Parere 3/2010 sul principio di responsabilità

13 luglio 2010 [doc. *web* n. 1791970]

WP 174 - Parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel *marketing* diretto

13 luglio 2010 [doc. *web* n. 1791975]

WP 175 - Parere 5/2010 sulla proposta dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni *RFID*

13 luglio 2010 [doc. *web* n. 1791979]

WP 176 - FAQ sulle questioni relative all'entrata in vigore della Decisione della Commissione 2010/87/EU del 5 febbraio 2010 sulle *standard contractual clauses* per il trasferimento dei dati ai responsabili stabiliti in Paesi terzi

12 luglio 2010 [doc. *web* n. 1791983]

WP 177 - Parere 6/2010 sul livello di protezione dei dati personali nella Repubblica orientale dell'Uruguay
12 ottobre 2010 [doc. *web* n. 1791988]

WP 178 - Parere 7/2010 concernente la Comunicazione della Commissione europea sull'approccio globale al trasferimento dei dati *PNR* verso Paesi terzi
12 novembre 2010 [doc. *web* n. 1791992]

WP 179 - Parere 8/2010 sulla legge applicabile
16 dicembre 2010 [doc. *web* n. 1791996]

Lettera del Gruppo Art. 29 al Commissario Karel de Gucht sulle implicazioni *privacy* dell'*Anti-Counterfeiting Trade Agreement* (*ACTA*)
15 luglio 2010 [doc. *web* n. 1792005]

Lettera del Gruppo Art. 29 alla Vicepresidente Viviane Reding sull'accordo tra UE e USA sulla protezione dei dati trasferiti e trattati a scopo di *law enforcement*
19 novembre 2010 [doc. *web* n. 1792013]

25.4. EUROPOL

Decisione 2009/371/GAI del Consiglio che istituisce l'Ufficio europeo di polizia (EUROPOL)
6 aprile 2009 (in vigore dal 1° gennaio 2010) [doc. *web* n. 1807328]

25.5. SISTEMA INFORMATIVO DOGANALE

Decisione 2009/917/GAI del Consiglio sull'uso dell'informatica nel settore doganale
30 novembre 2009 (in vigore dal 27 maggio 2011) [doc. *web* n. 1807332]

25.6. SCHENGEN

Rapporto dell'Autorità di controllo comune Schengen sul *follow-up* delle raccomandazioni riguardo all'impiego degli *alert* previsti dall'art. 96 nel Sistema informativo Schengen [doc. *web* n. 1808068]

25.7. 32MA CONFERENZA DELLE AUTORITÀ SU SCALA INTERNAZIONALE (GERUSALEMME, 27-29 OTTOBRE 2010)

Risoluzione sulla convocazione di una conferenza intergovernativa per adottare i princìpi internazionali in materia di *privacy*

29 ottobre 2010 [doc. *web* n. 1807350]

Risoluzione sulla "*Privacy by design*"

29 ottobre 2010 [doc. *web* n. 1807346]

25.8. *SPRING CONFERENCE* (PRAGA, 29-30 APRILE 2010)

Risoluzione relativa all'accordo UE-USA sugli *standard* nel settore di polizia e cooperazione giudiziaria

29-30 aprile 2010 [doc. *web* n. 1807235]

Risoluzione sul futuro della protezione dei dati e della *privacy*

29-30 aprile 2010 [doc. *web* n. 1807235]

Risoluzione sull'uso dei *body scanner* negli aeroporti

29-30 aprile 2010 [doc. *web* n. 1807235]

Risoluzione relativa ad azioni comuni sulla sensibilizzazione dei giovani a livello europeo ed internazionale

29-30 aprile 2010 [doc. *web* n. 1807235]

25.9. GRUPPO DI LAVORO IN MATERIA DI ATTIVITÀ GIUDIZIARIE E DI POLIZIA - *WPPJ*

Rapporto annuale di attività per l'anno 2009
[doc. *web* n. 1799280]

Raccomandazione in materia di misure attuative della Convenzione sulla criminalità informatica del Consiglio d'Europa
Praga, 29-30 aprile 2010 [doc. *web* n. 1799296]

Decisione sulla implementazione di una *policy* sulla supervisione europea
26 maggio 2010 [doc. *web* n. 1799292]

Documento sul Piano di azione della Commissione per l'implementazione del Programma di Stoccolma
13 ottobre 2010 [doc. *web* n. 1808075]

Documento sugli accordi bilaterali in ambito di polizia e cooperazione giudiziaria
15 ottobre 2010 [doc. *web* n. 1799288]

25.10. GRUPPO DI LAVORO INTERNAZIONALE SULLA PROTEZIONE DEI DATI NEL SETTORE DELLE TELECOMUNICAZIONI - *IWGDPT*

Documento di lavoro sul trattamento di dati attraverso dispositivi mobili e sicurezza
Berlino, 6-7 settembre 2010 [doc. *web* n. 1808545]

Documento di lavoro sull'utilizzo della *Deep Packet Inspection* a fini di *marketing*
Berlino, 6-7 settembre 2010 [doc. *web* n. 1808058]

Carta di Granada sulla *privacy* nel mondo digitale
Granada, 15-16 aprile 2010 [doc. *web* n. 1808062]

25.11. CONSIGLIO D'EUROPA

Raccomandazione (2010)13 sulla protezione dei dati personali in ambito di profilazione
23 novembre 2010 [doc. *web* n. 1807994]

Smartphone e tablet

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Smartphone e *tablet*: scenari attuali e prospettive operative

Schede di documentazione

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Francesco Pizzetti, *Presidente*
Giuseppe Chiaravalloti, *Vice Presidente*
Mauro Paissan, *Componente*
Giuseppe Fortunato, *Componente*

Daniele De Paoli, *Segretario generale*

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

Smartphone e tablet: scenari attuali e prospettive operative

PAGINA BIANCA

INDICE

PAGINA BIANCA

1. IL CONTESTO DELLE MOBILE APPS

1.1. Smartphone e tablet

Uno *smartphone* (o cellulare intelligente o telefono *touch*, cioè sensibile al tocco) è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer; esso, inoltre, impiega sensori per la determinazione della posizione (GPS) e per l'acquisizione di altri elementi dell'ambiente circostante l'utente. Le componenti *hardware* generalmente presenti in dispositivi di questo tipo sono riassunte in *Tabella 1*, le caratteristiche funzionali e la tipologia di destinazione d'uso sono rappresentate in *Tabella 2*:

Componenti trasmissive	Sensori e dispositivi
Modulo telefonico	Schermo *touch* inferiore ai 5"
Wifi (rete senza fili)	Altoparlante e microfono integrati
Bluetooth (rete senza fili)	Fotocamera/videocamera digitale
Radio FM	Dispositivo di localizzazione (GPS)
	Bussola digitale e altri sensori
	Moduli di pagamento

Tabella 1. Smartphone: caratteristiche + hardware di massima

Nuove caratteristiche
Applicazioni con funzionalità di localizzazione
Riconoscimento vocale, facciale e di immagini
Social network con possibilità di rendere nota la posizione geografica degli utenti
L'utente generalmente acquisisce applicazioni utilizzando lo specifico *market* dedicato (*OviStore* per *Nokia*, *Apple Store* per *Apple*, *Android Market* per *Google*, *Windows Market Place* per *Microsoft*)
Possibilità di confusione tra dati di origine diversa (es. quelli contenuti nella rubrica per uso personale e quelli relativi ai contatti di lavoro.)

Tabella 2. Smartphone: applicazioni innovative e nuove funzionalità delle applicazioni tradizionali

I *tablet* o *tablet computer* sono dispositivi assimilabili per componenti *hardware* e *software* agli *smartphone*, dai quali si distinguono per:

- dimensioni dello schermo
- possibile assenza del modulo telefonico
- destinazione d'uso

Gli *smartphone* e i *tablet computer* per lo più condividono la stessa infrastruttura tecnologica ovvero le stesse componenti *hardware* e lo stesso sistema operativo. I *tablet* sono però caratterizzati da uno schermo di dimensioni maggiori, il che li rende più idonei al consumo di prodotti multimediali ed editoriali (es. *gaming on-line*, *film on-demand*, abbonamenti a riviste e quotidiani) e meno pratici per essere utilizzati come telefoni e come PIM (*Personal Information Management*); per questa ragione alcuni esemplari non sono dotati di modulo telefonico. La maggior parte dei modelli si avvale, tuttavia, di schede SIM per la connessione dati con le tecnologie cellulari (GPRS e UMTS).

È opportuno osservare che, per le finalità connesse alle problematiche relative alla protezione dei dati personali, sia i dispositivi *tablet* che *smartphone* possono essere considerati unitariamente, dal momento che le modalità di funzionamento delle applicazioni sono pressoché identiche. Va altresì evidenziato che non costituisce oggetto di indagine l'impiego di questi dispositivi come apparecchi telefonici per le comunicazioni interpersonali.

1.2. Le mobile apps e i market

Per *mobile apps* o applicazioni per *smartphone* si intende il *software* che è possibile installare sugli *smartphone* e sui *tablet* per fornire funzionalità aggiuntive. Le applicazioni per *smartphone* estendono, cioè, le funzionalità rese disponibili dal sistema operativo dello specifico produttore e sono reperibili tramite *download* da una speciale applicazione che acquisisce il marchio (*brand*) del produttore del telefono o del sistema operativo installato sul telefono. Tale particolare applicazione viene

detta *market* ed è denominata diversamente dai vari produttori. I principali *market* attualmente sono:

- *Android Market* (*Google*)
- *Apple Store* (*Apple*)
- *Windows MarketPlace* (*Microsoft*)
- *Nokia Ovistore* (*Nokia*)

Tutti i *market* sono una speciale applicazione per *smartphone* che visualizza una vetrina virtuale dalla quale è possibile acquisire ulteriori applicazioni.

1.3. Smartphone e sistemi tradizionali: cosa cambia

Tablet e *smartphone* si differenziano dai *netbook* e dai *notebook* più tradizionali non soltanto per la specificità dell'*hardware* e del *software* di base, ma anche e soprattutto per i meccanismi e le modalità di acquisizione e distribuzione del *software* (*software acquisition* & *distribution*), che sono centralizzati e normalmente controllati dal fornitore del dispositivo, dall'operatore telefonico, dal produttore del sistema operativo o, infine, dal *"gestore del market"* che opera da intermediario tra il produttore/sviluppatore dei software e dei servizi (nella maggior parte dei casi esterno alla società e, dunque, terzo rispetto ad essa) e l'utente finale. Infatti, con specifico riguardo a *smartphone* e *tablet*, l'utente acquista *software* aggiuntivi (es. un videogame) e servizi (es. un cruscotto dell'andamento titoli, un servizio di condizioni meteo, un film in *streaming*, un *videogame* in *multiplayer*) avvalendosi di un'applicazione fornita dal gestore denominata *market* e preinstallata sul dispositivo.

Come sopra accennato, si tratta di una sorta di vetrina dei *software* e dei servizi disponibili resa accessibile all'utente per ampliare le funzionalità *software* del proprio *smartphone*. Il relativo utilizzo richiede la preventiva registrazione dell'utente e l'accettazione, da parte di quest'ultimo, delle condizioni contrattuali prefissate dal gestore del *market*, cristallizzate in un documento denominato *terms of service* (*ToS*).

In linea di massima non è possibile acquisire un'applicazione tramite canali tradizionali (es. CD acquistato in negozio), né avvalersi di modalità alternative a quelle

rigidamente previste dal gestore dello specifico *market* di riferimento, che va considerato lo strumento privilegiato e più diffuso per la distribuzione e l'acquisizione delle applicazioni per *smartphone*. L'eventuale installazione di applicazioni al di fuori del *market* è da ritenersi, dunque, una possibilità residuale.

Parallelamente, anche uno sviluppatore terzo che intenda creare un'applicazione in ambito *mobile* sarà tenuto ad accettare i *ToS* definiti dal detentore della piattaforma da lui scelta, ovvero dal gestore del *market*, e potrà vendere il suo prodotto solo attraverso il canale previsto da quest'ultimo.

Va sottolineato che il panorama delle *mobile apps* è molto vivace e in rapida evoluzione, anche in considerazione del fatto che le tecnologie alla base delle *mobile apps* (quali l'introduzione dei citati sensori sugli *smartphone*, la nuova modalità *touch* di interfacciamento con lo strumento), la facilità di accesso e di utilizzo di questi dispositivi e le innovative modalità di distribuzione dei relativi servizi hanno aperto la via a nuove, concrete opportunità di *business*, all'implementazione tecnologica ed alla diffusione di servizi ed applicazioni del tutto impensabili solo fino a qualche tempo fa. Attualmente esistono numerosissimi sviluppatori in ogni parte del mondo, caratterizzati da dimensioni imprenditoriali anche molto limitate, a volte semplici appassionati individuali senza particolari ambizioni commerciali, i quali con bassissimi investimenti e puntando su un'idea o un'intuizione creano e, attraverso la vetrina resa disponibile dal gestore (il *market*), mettono a disposizione di un mercato potenzialmente mondiale soluzioni talvolta molto innovative, in genere dal costo anche molto contenuto, che l'utente può acquistare in tutta semplicità, autonomia ed immediatezza. È tuttavia presumibile che questa dimensione artigianale con il tempo tenderà ad evolversi, convergendo verso una contrazione del numero degli sviluppatori che assumeranno connotazioni di maggior strutturazione e di più ampie dimensioni: è, infatti, verosimile che le aspettative dei consumatori siano destinate a crescere, con l'effetto che i prodotti, per essere competitivi, dovranno essere progressivamente più complessi e diversificati, con conseguente aumento dei costi di ideazione e sviluppo.

2. L'INDAGINE CONOSCITIVA

2.1. L'attività istruttoria

Agli inizi del 2011 l'Autorità ha avviato un'indagine che ha avuto come interlocutori privilegiati i principali produttori di sistemi operativi per *smartphone* (nello specifico, *Nokia*, *Microsoft*, *Apple*, *Google*), al fine di verificare gli accorgimenti adottati da queste società per garantire la sicurezza nell'utilizzo delle *mobile apps* sviluppate per i loro sistemi.

In particolare, le società sono state invitate ad indicare:

1. i meccanismi adottati o i requisiti richiesti (in termini, ad esempio, di affidabilità o di adeguato rispetto di misure di sicurezza) per selezionare preventivamente gli sviluppatori terzi (quelli, cioè, non direttamente dipendenti dalla società) autorizzati a distribuire le *application* di propria creazione sulle piattaforme di *market* di quest'ultima e quali condizioni e procedure siano previste per un'eventuale revoca dell'autorizzazione;

2. i meccanismi adottati per valutare le diverse funzionalità delle *application* e per verificare se la raccolta di dati personali effettuata dallo sviluppatore, per il tramite dell'applicazione, sia effettivamente pertinente rispetto alle predette funzionalità e alle finalità della raccolta;

3. le *policies* interne per assicurare il rispetto della normativa in materia di protezione dei dati personali e quali meccanismi siano adottati per verificare la conformità delle *application* già distribuite alla predetta normativa, nel caso in cui pervengano segnalazioni da parte degli utenti.

2.2. Riscontri pervenuti

Le risposte rese dai soggetti interpellati hanno evidenziato l'adozione di politiche aziendali solo in parte comuni.

In tutti e quattro i casi oggetto di indagine, ad esempio, lo sviluppatore terzo può proporre le applicazioni di propria creazione per la distribuzione sulla piattaforma di *market* dell'intermediario prescelto soltanto a seguito del perfezionamento di una

procedura di registrazione ed all'accettazione di specifici accordi contrattuali predisposti, proprio, da quest'ultimo; ne consegue una marcata eterogeneità delle clausole contrattuali cui gli sviluppatori sono vincolati, a seconda che decidano di proporre le proprie creazioni all'una o all'altra delle quattro diverse società.

Le indicazioni fornite, segnate naturalmente dal carattere della confidenzialità, hanno evidenziato differenze più o meno sensibili anche in ordine alle attività di controllo, alle assunzioni di responsabilità, ai rimedi esperibili in caso di inconvenienti, sia di carattere tecnico, nel funzionamento dell'applicazione, sia di carattere giuridico e dunque maggiormente attinenti agli aspetti contrattuali.

Ulteriori diversità sono state osservate anche con specifico riguardo al profilo che più direttamente interessa questa Autorità, quello cioè della protezione dei dati personali degli utenti. In quest'ambito è stato possibile, tuttavia, identificare due diversi e contrapposti modelli di condotta, che si distinguono per il modo in cui viene garantita la sicurezza delle applicazioni messe in vendita tramite il *market* e possono essere definiti nel modo seguente:

- *privacy by process*
- *privacy by platform*

Nel modello *privacy by process*, il processo di accreditamento dei potenziali sviluppatori e di inserimento delle loro applicazioni nel *market* viene sottoposto ad un rigido controllo, tipicamente formalizzato in un accordo *ToS* (*Terms of Service* - condizioni di contratto) tra il soggetto interessato a pubblicare il suo *software* sul *market* e il gestore del *market* stesso. Inoltre, l'applicazione viene controllata allo scopo di garantirne la sicurezza sotto il profilo tecnico prima dell'immissione nel mercato.

Nel modello *privacy by platform* il gestore del *market* non effettua un controllo preventivo sull'applicazione, ma affida la tutela dei diritti dell'utente alla solidità della piattaforma di sistema operativo, alle sue funzionalità che permettono all'utente di avere coscienza di quali dati saranno oggetto di trattamento da parte dell'applicazione disponibile sul *market*, facendo ricorso a meccanismi di *ranking* gestiti dagli

stessi utenti. In termini più concreti, chi utilizza il *market* può verificare per ogni applicazione disponibile le opinioni di coloro che prima di lui ne hanno già fatto uso, espresse sotto forma di punteggi sintetici e commenti. Inoltre, all'atto dell'installazione di un'applicazione la piattaforma *software* presente sul suo *smartphone* provvede ad informare l'utente su quali funzionalità l'applicazione utilizzerà e quindi a quali dati può potenzialmente accedere.

3. ASPETTI CRITICI LEGATI ALL'UTILIZZO DEGLI *SMARTPHONE*

La diffusione dei moderni *smartphone* determina una crescita sostenuta nell'utilizzo delle applicazioni per questo tipo di dispositivi: i principali *market* hanno ormai un *portfolio* che può superare le decine di migliaia di *apps*.

Gli utenti tendono a delegare la gestione di molti aspetti della propria vita sia personale che professionale alle nuove tecnologie, le quali fanno sempre più spesso impiego di informazioni relative alla geolocalizzazione degli interessati. Questi dati non sempre restano archiviati esclusivamente sul dispositivo, ma vengono frequentemente conservati in aree remote potenzialmente accessibili anche da altri utenti. Uno stesso *smartphone* può essere utilizzato per le finalità più disparate, ad esempio per la gestione del *portfolio* clienti, del catalogo e del calendario aziendali, ma anche per la condivisione di foto, informazioni, video etc. con i propri amici o familiari, per il confronto dei prezzi dei prodotti al supermercato con quelli del negozio *on-line*, per monitorare i propri movimenti bancari, per localizzare la propria autovettura in caso si dimentichi dove è stata posteggiata, per sapere, in quel determinato momento, chi dei propri amici si trovi in zona, per redigere programmi di benessere alla stregua delle proprie abitudini alimentari, per impostare il monitoraggio ormonale del ciclo femminile, e magari, in una prospettiva di prossima, futura realizzazione, persino come telecomando per aprire il cancello automatico del proprio box auto o per sbloccare la serratura della propria abitazione. Il ventaglio delle applicazioni possibili è, allora, realmente impressionante e destinato

ad accrescersi ulteriormente. Tuttavia, l'utilizzo di tali applicazioni implica l'elaborazione e quindi il trattamento di dati, anche personali, riservati e persino sensibili. In molti casi i dati verranno archiviati e conservati sul dispositivo, ma sempre più spesso ci si avvale di *mobile apps* che consistono in realtà in servizi erogati in modalità *web*, il cui utilizzo implica, cioè, che le informazioni personali siano spostate o copiate nella *cloud* del fornitore del servizio. Il fornitore, ovvero lo sviluppatore delle *mobile apps*, può essere lo stesso gestore del *market* o uno sviluppatore indipendente. In altri termini, molte delle applicazioni per *smartphone* sono servizi erogati in modalità *cloud* (*"Saas" - Software as a service*) che trasportano tutti o parte dei dati dell'utente nella *cloud*.

La transizione dal modello applicativo tradizionale a quello in cui il *software* è un servizio della *cloud* è condivisa sia dal fornitore sia dal consumatore, in quanto la modalità *cloud* costituisce apparentemente un'esclusiva facilitazione per l'utente. In realtà questi non è, spesso, neppure consapevole del fatto che sta utilizzando un servizio *cloud*; è, tuttavia, perfettamente al corrente della possibilità di accedere agli stessi dati da dispositivi differenti (*es. smartphone* e pc da scrivania) ovvero che se acquista uno *smartphone* nuovo può ritrovare, *"come per magia"*, tutti i propri dati sul nuovo dispositivo senza dover ricorrere a tediose transizioni dal vecchio al nuovo telefonino (si pensi allo spostamento dei contatti della rubrica).

Un ulteriore aspetto che viene proposto e percepito come facilitazione a valore aggiunto è l'integrazione di *set* di dati che hanno origini differenti. Ad esempio con i telefoni basati sul *software* di *Google* (*Android*) è possibile trasferire nella rubrica dello *smartphone* i contatti, compresi quelli di posta elettronica, prelevati dall'*account* Google. Inoltre alcuni produttori di telefoni danno la possibilità all'utente di integrare tale rubrica con ulteriori dati prelevati dal proprio *account Facebook*, aggiungendo ad esempio le foto e gli indirizzi di residenza.

Questi, in sintesi, gli aspetti critici di carattere generale in merito all'utilizzo della nuova generazione dei dispositivi *smartphone*:

• sono dispositivi pervasivi, utilizzabili in tutti gli aspetti della vita personale e professionale;

• è presumibile che vi si farà sempre più frequentemente ricorso per gestire anche dati "riservati";

• le facilitazioni d'uso favoriscono l'esternalizzazione dei dati;

• le facilitazioni d'uso favoriscono l'integrazione di dati tra aspetti distinti della propria vita (es. rubrica lavorativa e amici su *Facebook*).

3.1. Rischi e minacce specifici

Le precedenti osservazioni consentono, allora, di definire, elencandoli, i principali fattori connessi all'utilizzo dei sistemi *mobile* idonei a determinare rischi e minacce specifici per la protezione dei dati personali degli utenti. Segnatamente:

• la linea di demarcazione che permette di distinguere l'*Identità digitale* dall'*Identità reale* tende progressivamente ad affievolirsi sino a scomparire. L'utilizzatore di *applications* per *smartphone* è, infatti, identificabile abbastanza facilmente attraverso informazioni obiettive e concrete, non autonomamente modificabili (ad esempio il numero di telefonino, il codice IMEI, i dati anagrafici dei contatti registrati nella rubrica archiviata sul proprio dispositivo etc.);

• il *social networking* tende ad essere sempre più pervasivo e si integra e arricchisce con nuove informazioni personali (ad esempio la posizione geografica dell'utente);

• in generale, a causa dell'integrazione dei servizi informatici e dello scambio di dati tra applicazioni, telefono e servizi, è sempre più difficile - e spesso impossibile - controllare il flusso dei propri dati personali;

• a causa della progressiva diminuzione del controllo sui propri dati e della correlata fusione tra l'identità digitale e quella reale, emergono maggiori pericoli dal punto di vista della sicurezza informatica e si creano nuovi rischi e minacce

(es. *stalking* sociale, intercettazioni, furto di *account* di pagamento);

• possibilità di accedere da parte delle applicazioni a dati e strumenti in un modo ancor più invasivo che in passato (numero di telefono, rubrica, messaggi);

• possibilità da parte delle applicazioni di intrecciare aspetti differenti della vita degli utenti (es. vita privata e vita professionale) in modi non sempre chiari, conoscibili, prevedibili, controllabili e desiderati da parte dell'utente stesso;

• tracciamento e profilazione dell'utente a sua insaputa e disponibilità di dati univoci (IMEI, numero di telefono) da utilizzare ad esempio per la pubblicità comportamentale, per l'enforcement di un accordo di servizio o per la tutela del diritto d'autore;

• alcuni produttori, per ragioni di mercato, tendono a non distribuire tempestivamente gli aggiornamenti *software* che risolvono accertate vulnerabilità di sicurezza informatica.

In un tentativo di ulteriore schematizzazione, i rischi e le minacce in cui un utente può incorrere per un uso non accorto o non regolamentato delle *mobile apps* derivano da:

• mancanza di TRASPARENZA nelle modalità e nelle finalità di raccolta dei dati;

• incapacità o impossibilità da parte degli interessati di esercitare o recuperare il CONTROLLO sui propri dati e sul modo in cui essi vengono comunicati a terzi;

• elementi tecnici di SICUREZZA INFORMATICA

Trasparenza	Controllo	Sicurezza informatica

Tabella 3: Le tre dimensioni della protezione dei dati personali nelle apps

4. COME AUMENTARE LE GARANZIE PER GLI UTENTI

In questa sede si intendono formulare proposte di carattere operativo tese a favorire sia l'utilizzo consapevole, da parte dell'utente, degli strumenti e dei dispositivi dei quali si tratta, sia un più efficace esercizio dei propri diritti in merito alla gestione dei dati personali.

È opportuno muovere da una duplice considerazione:

- i produttori di dispositivi e dei relativi *software*, così come gli operatori di telefonia che commercializzano tali dispositivi previa apposizione del proprio marchio (*brand*), rivestono un ruolo importante sul livello di sicurezza dei dispositivi *mobile* che distribuiscono; coerentemente, sono loro i soggetti deputati a garantire anche la messa a disposizione di aggiornamenti tempestivi qualora siano rilevate nuove minacce per la sicurezza informatica. A questo riguardo, giova specificare che le caratteristiche del sistema operativo associato ad uno specifico dispositivo mutano a seconda che l'operatore di telefonia vi abbia apposto il proprio *brand* oppure no e sono, dunque, soggette ad una sorta di "personalizzazione" legata, proprio, al *brand*. In termini più concreti, la configurazione del *software* di un dispositivo destinato ad essere commercializzato previa apposizione di un marchio (per esempio *Telecom Italia*, *Vodafone*, *Wind*, *H3G* etc.) è almeno in parte determinata dall'operatore di telefonia stesso, con l'obiettivo di renderne l'utilizzo il più possibile idoneo alla fruizione dei servizi che esso stesso mette a disposizione dei propri clienti. Ne consegue che due telefonini originariamente ed apparentemente identici, poiché dello stesso modello e della stessa marca, potranno in realtà differenziarsi in maniera anche significativa sotto il profilo delle caratteristiche del *software* a seconda del gestore che ne curi la personalizzazione e vi apponga il proprio *brand*. In questa ipotesi, le mutate caratteristiche del *software* di un dispositivo cui sia stato apposto il marchio dell'operatore di telefonia potrebbero, in alcuni casi, influire sul processo di aggiornamento del *software* reso disponibile dal produttore del telefonino (ad

esempio *Nokia*, *Sony Ericsson*, *Samsung*, *LG* etc.), rendendolo non direttamente ed immediatamente fruibile;

- nel caso delle *mobile apps*, a differenza del tradizionale modello di acquisizione del *software* su PC, c'è generalmente - lo si ribadisce - un intermediario univoco che si frappone tra lo sviluppatore / fornitore del servizio e l'utente finale; in altri termini, l'indeterminata molteplicità degli sviluppatori da un lato e l'altrettanto enorme massa degli utenti dall'altro trovano il loro punto di contatto e di raccordo proprio per il tramite di pochi soggetti, appunto gli intermediari, sulle cui attività imprenditoriali e commerciali si concentra il funzionamento del peculiare mercato di riferimento.

Il panorama prevalente consente, allora, di ipotizzare interventi mirati che, sfruttando la posizione di centralità degli intermediari all'interno della richiamata dialettica contrattuale e di *business*, possano efficacemente raggiungere la maggior parte dei soggetti coinvolti, con il dichiarato intento di porre le basi di una disciplina chiara ed efficace di tutela degli utenti in materia di protezione dei dati personali che non costituisca, tuttavia, un limite né dal punto di vista della logica concorrenziale propria del mercato né tantomeno abbia l'effetto di imbrigliare le potenzialità creative degli sviluppatori delle più moderne tecnologie.

In questa prospettiva, giova sottolineare che proprio all'intermediario, cioè al gestore del *market* che è spesso anche il produttore del sistema operativo dello *smartphone*, compete sempre un potere definitivo segnato dal massimo carattere della deterrenza, e cioè quello di interdizione nei confronti del *software* prodotto da terze parti con le quali sussista un vincolo di carattere contrattuale.

Una prima conclusione: è indispensabile, perché gli utenti siano posti nella condizione di decidere con responsabilità in ordine all'utilizzo dei propri dati, agire in modo da accrescerne la consapevolezza sulle opportunità, ma anche sui potenziali rischi riconducibili al mondo degli *smartphone* e delle *mobile apps*.

È altrettanto fondamentale che gli utenti, dopo aver conferito e, in senso lato, affidato i propri dati, ne mantengano comunque il controllo.

Ed è proprio da queste considerazioni ed in questa direzione che l'Autorità intende muovere per affrontare la sfida offerta dal sempre più diffuso impiego di applicazioni per *smartphone*, adoperandosi concretamente - se del caso, anche mediante mirate campagne informative - per diffondere tra gli utenti una nuova cultura che tenga conto, oltre che delle affascinanti ed innovative possibilità rese accessibili dalle nuove tecnologie, anche di alcuni punti di particolare rilievo e delicatezza. Tra questi:

- il rischio cagionato dalla carenza di consapevolezza dell'utente in ordine a profili di assoluta rilevanza che lo riguardano in maniera diretta e possiedono potenziali attitudini lesive dei suoi diritti in materia di protezione dei dati personali;
- le specificità legate all'utilizzo di applicazioni, specie quelle ad opera di sviluppatori terzi, che raccolgono dati sulla vita privata (dai contatti alla posizione geografica, sino alle abitudini di consumi e comportamenti, a dati relativi alla salute ed alla vita di relazione);
- la possibilità che i soggetti che trattano le informazioni personali degli utenti, anche eventualmente di carattere sensibile, possano renderle "pubbliche" ovvero comunicarle ad altri soggetti determinati, sia per finalità commerciali che di altro genere, non specificamente correlate alla raccolta e, più in generale, non conformi ai desideri dell'utente medesimo, innanzitutto per l'indubbia attitudine dei dati a favorire attività di profilazione dell'utente;
- la possibilità che, in assenza di regole specifiche, i dati così raccolti possano essere archiviati sui sistemi del fornitore del servizio applicativo per periodi di tempo ultronei rispetto alla fornitura del servizio stesso, potenzialmente indeterminati; che, addirittura, possano continuare a costituire oggetto di trattamento perfino successivamente al momento in cui l'utente ha cessato di far ricorso ad una determinata applicazione ovvero di utilizzare uno specifico dispositivo.

Il duplice obiettivo di implementare sia la trasparenza nelle modalità di funzionamento delle applicazioni, con specifico riguardo al trattamento delle informazioni personali degli utenti, sia il controllo esercitabile, nonchè la dimensione

sovranazionale dei produttori e, in termini ancor più generali, il respiro globale del mercato delle *mobile apps,* suggeriscono di pensare alla possibile trasposizione degli interventi in un contesto più ampio di quello nazionale. Si potrebbe, cioè, ipotizzare un'azione sinergica con interlocutori, anche istituzionali, che operino in ambito comunitario.

Una prospettiva, questa, concretamente realizzabile, specie se si valuta lo specifico ruolo di mediazione assunto dai citati produttori di sistemi operativi che, essendo anche i gestori dei *market* ovvero dei cataloghi di applicazioni, hanno tra l'altro una capacità di interdizione nei confronti degli sviluppatori eventualmente inadempienti alle prescrizioni previste dalle disposizioni contrattuali (*Terms of Service*).

In tale quadro, più pregnanti garanzie per l'utente potranno essere ottenute attraverso una combinazione di accorgimenti tecnici - sufficientemente generali da non modificare le strategie di mercato ma comunque ragionevolmente efficaci - e di norme contrattualistiche da inserire negli accordi proposti dai gestori dei *market* e rivolti sia agli sviluppatori delle applicazioni che agli utenti finali.

Il futuro, insomma, è già incominciato.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cloud computing

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

Schede di documentazione

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Francesco Pizzetti, *Presidente*
Giuseppe Chiaravalloti, *Vice Presidente*
Mauro Paissan, *Componente*
Giuseppe Fortunato, *Componente*

Daniele De Paoli, *Segretario generale*

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

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

PAGINA BIANCA

INDICE

PAGINA BIANCA

1. PREMESSA

L'Autorità nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici, specie per quelli erogati tramite *cloud* pubbliche (*public cloud*), che comportano l'esternalizzazione di dati e documenti, ritiene opportuna e doverosa un'opera di informazione orientata a tutelare l'importante patrimonio informativo costituito dai dati personali.

Tali indicazioni si propongono, quindi, di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole o medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di *cloud computing* (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi.

Le avvertenze di seguito enucleate costituiscono un primo quadro di cautele che favoriscono il corretto trattamento dei dati personali attraverso l'utilizzo dei predetti servizi virtuali e, pertanto, si indirizzano anche ai fornitori, i quali possono fare riferimento a tali indicazioni nella predisposizione dei loro servizi, con l'accortezza di informare opportunamente gli utenti in ordine alla loro adozione.

L'Autorità - nella consapevolezza che l'utilizzo dei servizi di *cloud computing* prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale, e in considerazione di tutte le sue implicazioni in relazione al trattamento dei dati personali - intende in ogni caso continuare a seguire l'evoluzione del fenomeno, anche partecipando con altri decisori istituzionali a specifici tavoli di lavoro aperti in materia, in particolare con *DigitPA* per quanto attiene all'adozione di modelli orientati alle *cloud* in ambito pubblico. L'Autorità, inoltre, si riserva, laddove ne rilevasse la necessità, di adottare in futuro specifiche e dettagliate prescrizioni indirizzate a utenti e fornitori, specie sotto il profilo delle misure di sicurezza.

2. CHE COSA È IL *CLOUD COMPUTING*?

L'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione è inarrestabile e ogni giorno vengono messi a disposizione dei cittadini nuovi strumenti e soluzioni sempre più sofisticate e integrate con la rete Internet, che consentono di soddisfare crescenti esigenze di informatizzazione e di comunicazione.

In tale quadro, il *cloud computing* è un insieme di modelli di servizio che più di altri si sta diffondendo con grande rapidità tra imprese, pubbliche amministrazioni e cittadini perché incoraggia un utilizzo flessibile delle proprie risorse (infrastrutture e applicazioni) o di quelle messe a disposizione da un fornitore di servizi specializzato. L'innovazione e il successo delle *cloud* (le nuvole informatiche) risiede nel fatto che, grazie alla raggiunta maturità delle tecnologie che ne costituiscono la base, tali risorse sono facilmente configurabili e accessibili via rete, e sono caratterizzate da particolare agilità di fruizione che, da una parte semplifica significativamente il dimensionamento iniziale dei sistemi e delle applicazioni mentre, dall'altra, permette di sostenere gradualmente lo sforzo di investimento richiesto per gli opportuni adeguamenti tecnologici e l'erogazione di nuovi servizi.

Nell'ambito del *cloud computing* è ormai prassi consolidata distinguere tra *private cloud* e *public cloud.*

Una *private cloud* (o nuvola privata) è un'infrastruttura informatica per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell'*hosting* dei *server*) nei confronti del quale il titolare dei dati può spesso esercitare un controllo puntuale. Le *private cloud* possono essere paragonate ai tradizionali *"data center"* nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle attraverso investimenti contenuti e attuati progressivamente nel tempo.

Nel caso delle *public cloud*, invece, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni - e quindi condivide tra di essi - i propri sistemi attraverso l'erogazione

via *web* di applicazioni informatiche, di capacità elaborativa e di stoccaggio. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dell'elaborazione o dei soli dati presso i sistemi del fornitore del servizio, il quale assume un ruolo importate in ordine all'efficacia delle misure adottate per garantire la protezione dei dati che gli sono stati affidati. In questo caso l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi. Ad esempio, la complessità delle infrastrutture, e la loro eventuale dislocazione su siti al di fuori dei confini nazionali potrebbe determinare l'impossibilità sia di conoscere con esattezza l'ubicazione dei propri dati nella nuvola, sia di sapere se e quando i dati vengono spostati da un luogo all'altro per esigenze organizzative, tecniche o economiche difficilmente determinabili e gestibili a priori. Inoltre, la dimensione del fornitore potrebbe condizionare la forza contrattuale dei fruitori del servizio e la loro possibilità di esercitare un controllo diretto, seppur concordato, sui siti e sulle infrastrutture utilizzate per ospitarne i dati.

Acquisire servizi *cloud* significa acquistare presso un fornitore di servizio risorse (ad esempio *server* virtuali o spazio disco) oppure applicazioni (ad esempio posta elettronica e strumenti per l'ufficio)
• I dati non risiedono più su *server* "fisici" dell'utente, ma sono allocati sui sistemi del fornitore (a meno di copie in locale)
• L'infrastruttura del fornitore del servizio è condivisa tra molti utenti per cui sono fondamentali adeguati livelli di sicurezza
• L'utilizzo del servizio avviene via *web* tramite la rete Internet che assume dunque un ruolo centrale in merito alla qualità dei servizi fruiti ed erogati
• I servizi acquisibili presso il fornitore del servizio sono a consumo e in genere è facile far fronte ad eventuali esigenze aggiuntive (ad esempio più spazio disco o più potenza elaborativa)
• Esternalizzare i dati in remoto non equivale ad averli sui propri sistemi: oltre ai vantaggi, ci sono delle controindicazioni che bisogna conoscere

Tabella: Aspetti chiave legati al cloud computing erogato tramite cloud pubbliche

Accanto alle *private* e *public cloud* si annoverano nuvole "intermedie" quali le *cloud* ibride (o *hybrid cloud*), caratterizzate da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da *cloud* pubbliche, e le *community cloud* in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

I potenziali vantaggi del *cloud computing* certamente possono promuovere la sistematizzazione delle infrastrutture, la riorganizzazione dei flussi informativi, la razionalizzazione dei costi e quindi in generale favorire nel caso sia del mondo imprenditoriale, sia della pubblica amministrazione servizi più moderni, efficienti e funzionali in linea con le esigenze di crescita di un moderno Sistema Paese. È d'altra parte assodato che il *cloud computing* non è un fenomeno temporaneo o una moda, ma il passo successivo dell'evoluzione nel modo in cui si utilizza la Rete Internet, che da strumento per la sola condivisione documentale (la pagina *web* resa disponibile dal sito *web* remoto) diviene la porta d'accesso alle risorse elaborative di un *provider* di servizi (l'applicazione resa disponibile in modalità *web*).

Questa trasformazione sta determinando una "modifica dei costumi" che è già in atto ed è più evidente nell'utenza individuale che più frequentemente, ma non sempre con completa consapevolezza anche dei possibili rischi derivanti dalle nuove tecnologie utilizzate, si avvale di servizi erogati da fornitori terzi (*public cloud*) per far fronte alle sue esigenze informative: l'utente *consumer*, infatti, utilizza i *social network* sui quali trasferisce abitualmente foto, informazioni, idee e opinioni, usa strumenti di elaborazione documentale via *web*, impiega gli *hard-disk* remoti per poter sempre disporre dei propri documenti da qualunque dispositivo e in qualunque luogo si trovi, si avvale delle applicazioni per i moderni smartphone sempre connessi ad Internet che tramite l'associazione delle informazioni di geolocalizzazione all'utente hanno aperto la strada a innovative funzionalità, anche in ambito sociale.

Risulta d'altra parte evidente come l'offerta degli operatori economici stia incalzando il mercato delle imprese e della Pubblica Amministrazione con soluzioni che incoraggiano l'acquisizione di servizi esternalizzati, utilizzando come volano verso

i nuovi investimenti la prospettiva di risparmi legati alla sostituzione o all'affiancamento degli *asset* per il trattamento delle informazioni tradizionalmente nel diretto possesso dell'utente, con soluzioni acquisite a consumo presso terzi.

È tuttavia opportuno evidenziare come il ricorso a quelle modalità che intrinsecamente promuovono l'utilizzo di servizi esternalizzati comportino anche la migrazione dei dati dai sistemi locali sotto il diretto controllo dell'utente, impresa o amministrazione ai sistemi remoti del *provider* di servizi.

3. ESTERNALIZZARE I DATI NELLE *CLOUD* PUBBLICHE

Come sopra delineato, le *public cloud* (o nuvole informatiche pubbliche) sono infrastrutture controllate da organizzazioni che le rendono disponibili a terzi attraverso la vendita di servizi a consumo. Lo spazio virtuale e la capacità di elaborazione della "nuvola" sono condivisi tra molti utenti, singoli o appartenenti a imprese o enti diversi che accedono a tali risorse dell'infrastruttura tramite l'utilizzo della rete Internet.

Più precisamente, con il termine *cloud computing* o semplicemente *cloud* nell'ambito di questo documento ci si riferisce a un insieme di tecnologie e di modelli di servizio che:

- favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via *web*;
- promuovono a seconda dei casi il trasferimento dell'elaborazione o della sola conservazione dei dati dai *computer* degli utenti ai sistemi del fornitore dei servizi.

La flessibilità e la semplicità con cui è possibile configurare i sistemi in *cloud* ne rende possibile un dimensionamento "elastico", attuato cioè secondo logiche di adattabilità alle contestuali esigenze e di fruizione a consumo. Gli utenti non devono curarsi della gestione dei sistemi informatici che, essendo utilizzati secondo la logica dell'esternalizzazione (*outsourcing*), sono completamente gestiti dai soggetti terzi nella cui nuvola sono conservati i dati. Generalmente, nel caso frequente di fornitori di grosse dimensioni dotati di infrastrutture complesse, la nuvola può estendersi

geograficamente su siti distinti e l'utente potrebbe ignorare dove vengono effettivamente conservati i propri dati.

I servizi offerti dai fornitori di soluzioni di *cloud computing* sono molto diversificati, in costante e significativo aumento e spaziano da sistemi elaborativi virtuali, che sostituiscono o si affiancano ai tradizionali elaboratori ubicati nei locali propri dell'organizzazione, a servizi di supporto allo sviluppo e per l'*hosting* evoluto delle applicazioni, sino a soluzioni *software* rese disponibili in modalità *web* che sono sostitutive delle tradizionali applicazioni installate sui computer di utenti, imprese e di amministrazioni, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, eventualmente condivisi, cartelle per l'archiviazione dei documenti *on-line*, e persino soluzioni esternalizzate di posta elettronica. I dati trasferiti e archiviati per mezzo di questi servizi *web* presso il *service provider* possono essere trattati dagli utenti in remoto attraverso la rete Internet spesso senza la necessità di installare specifici programmi sui propri sistemi e senza l'esigenza di dover effettuare gli aggiornamenti *software* e tutte le altre attività correlate alla manutenzione e alla gestione delle infrastrutture informatiche.

4. I DIVERSI MODELLI DI SERVIZIO

Sul mercato, a seconda delle esigenze dell'utente, sono disponibili varie soluzioni di *cloud computing* erogate secondo modalità che ricadono in linea di massima in tre categorie, dette "modelli di servizio". Comunemente tali modelli di servizio sono riferiti sia a soluzioni di *private cloud* che di *public cloud*, ma vengono qui illustrati in un'ottica maggiormente aderente a quest'ultima tipologia di servizi, che prevede l'utilizzo condiviso da parte di utenti, imprese e soggetti pubblici dei sistemi di *provider* di servizi terzi.

- Nel caso di servizi *IaaS* (*Cloud Infrastructure as a Service* - infrastruttura *cloud* resa disponibile come servizio), il fornitore noleggia un'infrastruttura tecnologica, cioè *server* virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione

o l'affiancamento ai sistemi già presenti nei locali dell'azienda. Tali fornitori sono in genere operatori di mercato specializzati che realmente dispongono di un'infrastruttura fisica, complessa e spesso distribuita in aree geografiche diverse.

• Negli *SaaS* (*Cloud Software as a Service - software* erogato come servizio della *cloud*), il fornitore eroga via *web* una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi, che è quindi spinto ad "esternalizzare" i suoi dati affidandoli al fornitore. Si pensi, ad esempio, ad applicazioni tipiche per l'ufficio erogate in modalità *web* quali fogli di calcolo, elaborazione dei testi, applicazioni per il protocollo informatico, la rubrica dei contatti e i calendari condivisi, ma anche alle moderne offerte di posta elettronica *cloud*.

• Infine, nei *PaaS* (*Cloud platform as a service* - piattaforme *software* fornite via *web* come servizio), il fornitore offre soluzioni per lo sviluppo e l'*hosting* evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di assolvere a esigenze interne oppure per fornire a loro volta servizi a terzi. Anche nel caso dei *PaaS* il servizio erogato dal fornitore elimina la necessità per il fruitore di doversi dotare internamente di strumenti *hardware* o *software* specifici o aggiuntivi.

5. INNOVARE, GOVERNANDO I RISCHI

L'utilizzo di servizi di *cloud computing* è un fenomeno in forte ascesa e determina un cambio di mentalità nelle modalità di utilizzo della rete Internet che, da strumento di condivisione documentale, diviene la porta di accesso alle risorse elaborative e di stoccaggio di fornitori di servizi remoti.

Tale tipologia di servizi comporta la migrazione di dati dai sistemi locali sotto il diretto controllo dell'utente ai sistemi remoti del fornitore, che assume un ruolo

centrale in ordine alla sicurezza dei dati e, quindi, all'adozione delle misure necessarie a garantirla. Tuttavia, è bene evidenziare come l'adozione di servizi esternalizzati non esime le imprese e le amministrazioni pubbliche che se ne avvalgono per la gestione del proprio patrimonio informativo dalle responsabilità che vengono loro attribuite, in particolare, dalla disciplina in materia di protezione dei dati personali.

I trattamenti di dati personali richiedono, infatti, sempre un'attenta ponderazione dei rischi legati alla sicurezza e alla fruibilità delle informazioni, indipendentemente dalle modalità di trattatamento. Pertanto, vanno tenute in debito conto le particolari caratteristiche delle nuove tecnologie, allo scopo di governare i potenziali pericoli che possono derivare da utilizzi scarsamente consapevoli e da modelli innovativi adottati con metodi, prassi e processi non ancora sufficientemente consolidati e in grado di mitigare le eventuali criticità. È quindi opportuno, anche nel caso del *cloud computing*, razionalizzarne le peculiarità al fine di individuare i potenziali rischi insiti in tali servizi e quindi poter adottare efficaci e specifiche misure di prevenzione.

Nel caso del *cloud computing*, il trasferimento dei dati dai computer locali, nella fisica disponibilità e nel diretto controllo esercitabile dal titolare, verso sistemi remoti di proprietà di un terzo fornitore del servizio, presenta, accanto a potenziali utilità, anche i seguenti aspetti che necessitano di specifica attenzione:

- l'utente, affidando i dati ai sistemi di un fornitore remoto, ne perde il controllo diretto ed esclusivo; la riservatezza e la disponibilità delle informazioni allocate sulla nuvola certamente dipendono anche dai meccanismi di sicurezza adottati dal *service provider*;
- il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri *service provider*, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati;

• il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali quali, ad esempio, guasti, impedendo l'accessibilità temporanea ai dati in esso conservati;

• le *cloud* sono sistemi e infrastrutture condivise basate sul concetto di risorse noleggiate a un'utenza multipla e mutevole; i fornitori, infatti, custodiscono dati di singoli e di organizzazioni diverse che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza;

• la conservazione dei dati in luoghi geografici differenti ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra l'utente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati;

• l'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la transizione di dati e documenti da un sistema *cloud* ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi *cloud* di fornitori differenti, ponendone quindi a rischio la portabilità o l'interoperabilità dei dati.

Il fornitore, in base alla tipologia dei servizi offerti, assume la responsabilità di preservare la riservatezza, l'integrità o la disponibilità dei dati; pertanto, l'utente al momento della stipula dei contratti di servizio dovrà tenere in debito conto gli accorgimenti previsti per garantire il corretto trattamento dei dati immessi nella *cloud.*

Prima di adottare un sistema basato nel *cloud computing* è necessario, quindi, valutare attentamente il rapporto tra rischi e benefici derivante dall'utilizzo del predetto servizio virtuale, minimizzando i primi attraverso una attenta verifica dell'affidabilità del fornitore di servizi al quale ci si intende affidare.

6. INDICAZIONI PER L'UTILIZZO CONSAPEVOLE DEI SERVIZI *CLOUD*

• *Ponderare prioritariamente rischi e benefici dei servizi offerti*

Prima di optare per l'adozione di servizi di *cloud computing*, è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (es. dati personali identificativi o meno, dati sensibili oppure particolarmente delicati come quelli genetici o biometrici, dati critici per la propria attività come ad esempio progetti riservati). E' necessario innanzitutto valutare gli eventuali rischi e le possibili conseguenze derivanti da tale scelta sotto il profilo della riservatezza e della loro rilevanza nel normale svolgimento della propria attività. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a servizi *cloud* (limitandone l'uso ad esempio a determinati tipi di dati), nonché l'impatto sull'utente in termini economici e organizzativi l'indisponibilità, pur se parziale o per periodi limitati dei dati esternalizzati o, peggio, la loro perdita o cancellazione.

• *Effettuare una verifica in ordine all'affidabilità del fornitore*

Gli utenti dovrebbero ragionevolmente accertare l'affidabilità del fornitore prima di migrare sui sistemi virtuali i propri dati più importanti, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare nella *cloud*, i rischi e le misure di sicurezza. In funzione della tipologia di servizio che necessitano, oltre che della criticità dei dati, è opportuno che valutino la stabilità societaria del fornitore, le referenze, le garanzi offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti. Gli utenti dovrebbero valutare, inoltre, le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità. Ulteriori criteri in base ai quali è possibile valutare l'affidabilità di un fornitore emergono dall'impiego di personale qualificato, dall'adeguatezza delle infrastrutture informatiche e di comunicazione, dalla disponibilità ad assumersi responsabilità, esplicitamente previste dal contratto di servizio, derivanti da

eventuali falle nel sistema di sicurezza o a seguito di interruzioni di servizio.

• *Privilegiare i servizi che favoriscono la portabilità dei dati*

E' consigliabile ricorrere a servizi di *cloud computing* nelle modalità SaaS, PaaS o IaaS in un'ottica lungimirante, vale a dire privilegiando servizi basati su formati e standard aperti, che facilitino la transizione da un sistema *cloud* ad un altro, anche se gestiti da fornitori diversi. Ciò al fine di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio da parte di uno qualunque degli operatori che intervengono nella catena di fornitura si traducano in condizioni peggiorative vincolanti o, comunque, per facilitare eventuali successivi passaggi da un fornitore all'altro.

• *Assicurarsi la disponibilità dei dati in caso di necessità*

Nell'utilizzo dei servizi di *cloud computing*, in assenza di stringenti vincoli sulla qualità formalizzati attraverso il contratto con il fornitore, si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente. Ciò specie quando ci si affidi a servizi gratuiti o a basso costo quali, ad esempio, a servizi di *hard-disk* remoto, *mail*, soluzione per la conservazione documentale e così via, che potrebbero non presentare adeguate garanzie di disponibilità e prestazioni tipiche, invece, dei servizi professionali. Certamente, nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (*backup*) dei dati allocati nella *cloud*, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo

di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità.

• *Selezionare i dati da inserire nella cloud*

Alcune informazioni che si intende inserire sui sistemi del fornitore di servizio, per loro intrinseca natura, quali ad esempio i dati sanitari, genetici, reddituali, biometrici o quelli coperti da segreto industriale, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella *cloud* consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di *cloud computing* oppure mantenere *in house* il trattamento di tali tipi di dati.

• *Non perdere di vista i dati*

E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore proponente, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo. Si pensi ad esempio a un applicativo in modalità *cloud* nel quale il fornitore del servizio finale (*Software as a Service*) offerto all'utente si avvalga di un servizio di stoccaggio dati acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nella *cloud* dall'utente.

• *Informarsi su dove risiederanno, concretamente, i dati*

Sapere in quale Stato risiedono fisicamente i *server* sui quali vengono allocati i dati, è determinate per stabilire la giurisdizione e la legge applicabile nel caso di

controversie tra l'utente e il fornitore del servizio. La presenza fisica dei *server* in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale. Non è, quindi, indifferente per l'utente sapere se i propri dati si trovino in un *server* in Italia, in Europa o in un imprecisato Paese extraeuropeo. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le *cloud* avvenga nel rispetto delle cautele previste a livello di Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

• *Attenzione alle clausole contrattuali*

Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. In ogni caso, è importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di *cloud* con riferimento ad obblighi e responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e di conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi da privilegiare la previsione di garanzie di qualità chiare, corredate da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti, ecc.). Si suggerisce, inoltre, di verificare eventuali soggetti terzi delegati alla fornitura di servizi intermedi e che concorrono all'erogazione del servizio finale rivolto all'utente, ovvero la preventiva identificazione dei diversi fornitori successivamente coinvolti nel trattamento. Si raccomanda, infine, di accertare quale sia la quantità di traffico dati prevista dal contratto oltre la quale vengono addebitati oneri economici supplementari.

• *Verificare le politiche di persistenza dei dati legate alla loro conservazione*

In fase di acquisizione del servizio *cloud* è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

• *Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati*

Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore per consentire l'allocazione dei dati nella *cloud*. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su *username* e *password*, purché le *password* non siano banali e vengano scelte di lunghezza adeguata. Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati - quali quelli sanitari, genetici, reddituali e biometrici o, più in generale, dati la cui riservatezza possa considerarsi "critica" - si raccomanda oltre all'utilizzo di protocolli sicuri nella fase di trasmissione, anche la conservazione in forma cifrata sui sistemi del fornitore di servizio.

• *Formare adeguatamente il personale*

Il personale preposto al trattamento di dati attraverso i servizi di *cloud computing* dovrebbe essere sottoposto a specifici interventi formativi, che evidenzino adeguatamente

le modalità più idonee per l'acquisizione e l'inserimento dei dati nella *cloud*, la consultazione e in generale l'utilizzo dei nuovi servizi esternalizzati e delle indicazioni sin qui illustrate, allo scopo di mitigare rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza: circostanze queste che potrebbero dare luogo ad accessi illeciti, perdita di dati o, più in generale, trattamenti non consentiti.