SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Doc. CXXXVI
n. 3

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(ANNO 2009)

(Articolo 154, comma 1, lettera m), *del decreto legislativo 30 giugno 2003, n. 196)*

Presentata dal Garante per la protezione dei dati personali

(PIZZETTI)

Comunicata alla Presidenza il 13 luglio 2010

TIPOGRAFIA DEL SENATO (50)

Doc. CXXXVI
n. 3

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(ANNO 2009)

(Articolo 154, comma 1, lettera m), *del decreto legislativo 30 giugno 2003, n. 196)*

Presentata dal Garante per la protezione dei dati personali

(PIZZETTI)

INDICE GENERALE

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

II. L'ATTIVITÀ SVOLTA DAL GARANTE

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

1. PRINCIPALI INTERVENTI DELL'AUTORITÀ NEL 2009

1.1. PROVVEDIMENTI PIÙ SIGNIFICATIVI

1.1.1. Trattamenti collegati allo svolgimento di funzioni di giustizia e di sicurezza pubblica

Nel corso del 2009 gli interventi del Garante in materia di giustizia e di sicurezza pubblica hanno riguardato profili relativi sia alla sfera internazionale sia a quella interna.

Nell'ambito dell'azione comune deliberata dall'Autorità di controllo Schengen (istituita dall'art. 115 della Convenzione di applicazione dell'Accordo di Schengen) volta ad accertare la liceità e la correttezza del trattamento dei dati da parte degli Stati membri a fini di sorveglianza discreta o di controllo specifico (art. 99 della Convenzione), il Garante ha svolto, ai sensi dell'art. 160 del Codice, presso i competenti uffici, centrali e periferici, del Ministero dell'interno-Dipartimento della pubblica sicurezza, accertamenti sulla liceità e correttezza dei trattamenti ivi effettuati in attuazione della Convenzione.

In esito a tali accertamenti l'Autorità, con *provvedimento* 12 novembre 2009, ha chiesto al citato Ministero un rafforzamento delle misure impiegate a tutela delle informazioni (segnalazioni su soggetti non appartenenti all'area Schengen, persone scomparse, estradizioni, notifiche di provvedimenti dell'autorità giudiziaria) trattate in applicazione dell'Accordo di Schengen, che prevede lo scambio delle medesime tra le banche dati delle forze di polizia dei paesi aderenti, al fine di garantire meglio la sicurezza delle frontiere.

Le misure prescritte attengono, in sintesi, alla tracciabilità degli accessi al sistema informatico, che devono basarsi su procedure certificate, su cui dovrà vigilare un'unità di *auditing* potenziata e responsabile della sicurezza dei dati.

Analoga accortezza dovrà essere adottata per garantire i flussi informativi della Divisione SIRENE che raccoglie, dal Centro elaborazione dati (Ced) del Dipartimento di pubblica sicurezza e dagli uffici di polizia interessati, le informazioni aggiuntive ritenute utili a dare seguito alle segnalazioni e le trasmette agli uffici dell'omologa Divisione del Paese in cui il soggetto è stato rintracciato.

La sala *server* delle Divisioni N-SIS e SIRENE dovrà essere protetta mediante l'adozione di una procedura speciale di *strong authentication*, ottenuta dalla combinazione di più credenziali di accesso (*badge* nominativo e dispositivo basato su una caratteristica biometrica); dovrà inoltre essere garantita la disponibilità e la continuità di esercizio della banca dati adottando piani di prevenzione che impediscano la sospensione dei servizi.

Con *provvedimento* 10 settembre 2009 [doc. *web* n. 1658464] il Garante ha altresì espresso parere favorevole su uno schema di Protocollo d'intesa tra il Ministero dell'interno e il Ministero della giustizia, relativo alla trasmissione telematica delle notizie di reato e degli esiti dei procedimenti penali ad esse connessi tra il Ced del Dipartimento di pubblica sicurezza e le procure della Repubblica.

Il Protocollo disciplina la collaborazione tra le due amministrazioni per dare attuazione al progetto denominato "Notizie di Reato1" (NdR1), volto a migliorare l'efficienza e la rapidità nell'acquisizione delle notizie di reato da parte delle procure e ridurre i tempi di trasmissione delle informazioni relative alle conclusioni dei procedimenti penali dalle procure alle forze di polizia.

Ciò potrà favorire un più rapido e puntuale aggiornamento dei dati personali trattati presso il Ced, nel rispetto dei requisiti di esattezza e completezza.

Il *parere* tiene conto dei chiarimenti forniti dai due ministeri nel corso di alcuni incontri tecnici tenuti presso l'Autorità, che hanno riguardato, in particolare, gli aspetti del progetto relativi alla corretta identificazione delle parti che comunicano fra loro (forze di polizia e procure) e dei sistemi informatici (S.d.i. del Ced e Re.ge delle procure) che alimentano il flusso tra le amministrazioni; l'esclusiva disponibilità e gestione da parte delle procure delle notizie di reato trasmesse dalle forze di polizia;

la più analitica descrizione delle modalità di accesso e i tipi di informazioni "visibili" relative alle notizie di reato "segretate".

Si segnala altresì il *provvedimento* 16 dicembre 2009 [doc. *web* n. 1689683], con cui il Garante ha espresso parere favorevole, con condizioni, in ordine ad uno schema di decreto recante regole tecnico-operative sul processo civile telematico, in sostituzione del d.m. del 17 luglio 2008. Il Garante ha richiesto, in particolare, una più precisa definizione dei soggetti legittimati alla consultazione del sistema informativo civile, nonché misure volte a garantire la sicurezza dei dati e del sistema, con particolare riferimento alle procedure di controllo degli accessi - necessariamente selettivi - ed ai sistemi di autenticazione.

Per quanto riguarda la materia della sicurezza e dell'ordine pubblico, in data 28 maggio 2009 il Garante ha espresso *parere* [doc. *web* n. 1624697] favorevole, con osservazioni, in ordine a uno schema di accordo tra Italia e Usa per il contrasto di gravi forme di criminalità che prevede, tra l'altro, un rilevante flusso di dati personali tra gli organi investigativi dei due Paesi e l'accesso ai profili del Dna relativi a soggetti condannati o imputati di *"serious crimes"*. Il Garante ha suggerito al Governo, in particolare, di meglio precisare la tipologia delle *"gravi forme di criminalità"* il cui contrasto legittima lo scambio informativo dei dati, anche in ragione delle rilevanti difformità tra i sistemi penali italiano e statunitense federale; di perfezionare le norme suscettibili di legittimare il trattamento di dati personali per finalità estranee all'accordo e diverse da quelle per le quali i dati sono stati acquisiti; di migliorare la formulazione delle norme sull'accesso dell'interessato ai dati personali che lo riguardano, evitando il rischio di comprimere eccessivamente il controllo dell'interessato medesimo sul trattamento dei propri dati personali.

1.1.2. Trattamento dei dati di traffico telefonico e telematico

Nel periodo di riferimento ha avuto un seguito la questione riguardante i termini entro i quali i fornitori di servizi telefonici e telematici avrebbero dovuto conformare i propri sistemi alle misure e agli accorgimenti prescritti con il *provvedimento* del 17 gennaio 2008 [doc. *web* n. 1482111], integrato il 24 luglio 2008

[doc. *web* n. 1538224], di cui si è già dato conto nella *Relazione 2008*, p. 173.

Associazioni rappresentative del settore delle comunicazioni elettroniche, in ragione di un sostanziale, ma non ancora integrale, adeguamento alle prescrizioni ivi contenute hanno infatti richiesto di prorogare i termini.

L'Autorità, in ragione della complessità degli interventi a tal fine necessari, nonché della mole degli investimenti complessivi previsti e di quelli già impegnati, ha accordato - anche se limitatamente ad alcune misure specificamente indicate - la richiesta proroga. Pertanto, con *provvedimento* 29 aprile 2009 (in *G.U.* 11 maggio 2009, n. 107 [doc. *web* n. 1612508]), è stato fissato il nuovo termine del 15 dicembre 2009, richiedendo altresì a tutti i titolari del trattamento interessati, entro la medesima data, la conferma delle misure e degli accorgimenti adottati e l'attestazione dell'integrale adempimento.

1.1.3. Sicurezza e trasparenza dei dati relativi all'attività tributaria

Gli accertamenti svolti sul sistema informativo della fiscalità, per la rilevanza dei dati trattati e la forte incidenza sulla vita dei cittadini, hanno evidenziato l'esigenza di rafforzare le garanzie per gli interessati, in termini di correttezza dei trattamenti e di sicurezza dei sistemi.

La complessità delle banche dati e delle misure da porre in essere ha portato, in diversi casi, a prorogare i termini stabiliti in precedenza.

In questo quadro, con *provvedimento* 7 ottobre 2009 [doc. *web* n. 1664231], anche sulla base di accertamenti ispettivi, l'Autorità ha individuato una serie di prescrizioni per il trattamento di dati personali effettuato a fini di riscossione a mezzo ruolo, la cui gestione è stata ricondotta in capo all'amministrazione finanziaria, che la esercita mediante la società Equitalia e le altre società del gruppo, a seguito di una recente riforma.

Le prescrizioni impartite nell'articolato *provvedimento* riguardano, in sintesi: le sfere di competenza e le responsabilità dei predetti soggetti rispetto al trattamento dei dati, al fine di regolare con precisione le rispettive attribuzioni ed assicurare il corretto trattamento delle informazioni; l'esigenza di informare più chiaramente i contribuenti

sull'uso dei dati personali e di utilizzare dati indispensabili - eliminando quelli non necessari - e aggiornati, con tempi di conservazione strettamente correlati alle effettive esigenze; l'elevazione del livello di sicurezza per gli accessi ai diversi sistemi, con riferimento altresì agli accessi da parte degli enti locali - anche attraverso società esterne - ai fini della riscossione delle proprie entrate ai sensi dell'art. 83, comma 28-*sexies*, del d.l. 25 giugno 2008, n. 112.

L'Autorità ha prescritto, inoltre, all'Agenzia delle entrate e ad Equitalia l'adozione di idonee e concrete procedure di *audit*, anche periodiche, sugli accessi all'anagrafe tributaria effettuati a fini di riscossione, basate sul monitoraggio delle transazioni, nonché su verifiche periodiche - anche a campione - sull'attualità della pendenza soprattutto in relazione ai ruoli ante riforma. Tali controlli dovranno essere predisposti da Equitalia sulle attività svolte dalle società del gruppo e da Sogei.

Nel rispetto delle competenze attribuite dalla legge, il Garante ha impartito prescrizioni analoghe alla Regione Sicilia e alle società che si occupano della riscossione a mezzo ruolo sul territorio regionale.

Sempre per quanto attiene al delicato tema degli accessi al sistema, con *provvedimento* 26 marzo 2009 [doc. *web* n. 1605576], su richiesta dell'Agenzia, nel prorogare i termini per alcuni adempimenti, il Garante ha previsto che gli enti esterni abilitati ad accedere all'anagrafe tributaria attraverso i propri amministratori locali (deputati alla gestione delle utenze) accertino, sotto la propria responsabilità, l'attualità di ciascuna utenza attiva.

L'Autorità ha altresì previsto che i medesimi enti inibiscano gli accessi non riconducibili all'art. 19 del Codice (che rinvia a norme di legge o regolamento, nonché ad eventuali comunicazioni al Garante ai sensi del medesimo articolo) e quelli non conformi a quanto stabilito nelle apposite convenzioni, fornendo riscontro di tale verifica nel termine di novanta giorni, all'Agenzia, per la successiva disattivazione, da parte di questa, delle utenze non in uso agli amministratori locali che non siano state verificate.

Con altri *provvedimenti* (26 novembre 2009 [doc. *web* n. 1679426], 24 settembre 2009 [doc. *web* n. 1657692], 2 luglio 2009 [doc. *web* n. 1640373], 17 luglio 2009

[doc. *web* n. 1639318] e 23 luglio 2009 [doc. *web* nn. 1640317 e 1640349]) in relazione ai collegamenti all'anagrafe tributaria di alcuni enti (Inps, Inpdap, Enpals, Avcp, camere di commercio e Agea), sono stati prescritti misure e accorgimenti necessari a porre rimedio alle carenze riscontrate e ad incrementare i livelli di sicurezza degli accessi.

È stato prorogato da ultimo, con il menzionato *provvedimento* 26 novembre, l'utilizzo delle attuali modalità di accesso, allo scopo di garantire la continuità delle funzioni istituzionali perseguite dagli enti in parola mediante i collegamenti all'anagrafe tributaria; ciò fino al termine delle verifiche in corso su una nuova classe di *web services*, in via di sperimentazione, illustrata al Garante dall'Agenzia delle entrate.

1.1.4. Giornalismo - Dati di vittime di abusi. Persone e fatti d'interesse pubblico. Accessibilità online *di archivi storici dei quotidiani. Immagini tratte da* social network

Diversi profili dell'attività giornalistica, relativi al rapporto tra la libertà d'informazione e la protezione della sfera giuridica dei singoli, sono stati oggetto d'intervento del Garante nel periodo di riferimento.

Per quanto attiene al bilanciamento tra diritto di cronaca ed esigenza di protezione delle vittime di violenze, con i *provvedimenti* 28 gennaio 2010 [doc. *web* n. 1696265] e 11 febbraio 2010 [doc. *web* n. 1696239] l'Autorità ha dapprima bloccato e poi definitivamente vietato, nei confronti di diverse testate giornalistiche, ogni ulteriore diffusione, con qualsiasi mezzo, di informazioni idonee, anche indirettamente, a identificare una vittima di atti di violenza sessuale (nello stesso senso *cfr. Relazione 2008*, p. 7).

Nella specie la vittima, minorenne, pur non individuata nominativamente, era resa identificabile dalla diffusione di dettagliate informazioni relative ai soggetti ritenuti responsabili della violenza (quali le generalità di congiunti e di vicini di casa), nonché di dati relativi alla sua stessa persona (il luogo di abitazione, la composizione del nucleo familiare). Tale diffusione risultava in contrasto con l'art. 114, comma 6, del c.p.p., nonché, segnatamente, con l'art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'attività giornalistica [doc. *web* n. 1556386] che - anche attraverso il richiamo alla Carta di Treviso - considera sempre prevalente il diritto del minore alla riservatezza

rispetto al diritto di cronaca e vieta la diffusione di dati idonei ad identificare, anche indirettamente, minori comunque coinvolti in fatti di cronaca.

Per quanto riguarda immagini di personaggi famosi riprese in dimore private, sono stati vietati il trattamento e l'ulteriore diffusione sia delle immagini di un noto attore all'interno della sua villa (*Provv.* 18 giugno 2009 [doc. *web* n. 1623306]), raccolte superando fisicamente o con strumenti tecnologici una barriera visiva; sia delle immagini di una importante personalità politica, raccolte con un teleobiettivo all'interno del suo parco privato (*Provv.* 22 dicembre 2009 [doc. *web* n. 1686747]). In entrambi i casi, invece, non sono stati ravvisati profili di illiceità nel trattamento di immagini acquisite in luoghi pubblici o aperti al pubblico.

Di rilievo anche nel 2009 (*cfr. Relazione 2008*, p. 7) la tematica degli archivi storici *online* di giornali, con il contrasto tra l'interesse pubblico alla conoscenza di fatti seppur risalenti ed il diritto all'oblio vantato dagli interessati.

In alcuni casi, in considerazione del tempo trascorso e della inattualità di vicende risalenti, si è ritenuto che una persistente associazione all'interessato dei fatti conoscibili attraverso gli archivi storici *online* costituisca un sacrificio sproporzionato dei suoi diritti.

L'Autorità in alcuni provvedimenti ha stabilito pertanto che la pagina *web* contenente i dati personali dell'interessato (qual è il suo nominativo) sia sottratta alla diretta individuabilità tramite i comuni motori di ricerca, pur restando essa inalterata nel contesto dell'archivio e consultabile telematicamente accedendo all'indirizzo *web* dell'editore (*Provv.* 8 aprile 2009 [doc. *web* n. 1617673], *Provv.* 22 dicembre 2009 [doc. *web* n. 1695208], *Provv.* 15 gennaio 2009 [doc. *web* n. 1589209]); talvolta si è preso atto degli adempimenti in tal senso posti in essere dalla testata giornalistica titolare del trattamento dopo la presentazione del ricorso (*Provv.* 19 novembre 2009 [doc. *web* n. 1689109]).

Viceversa, in presenza di un persistente interesse pubblico alla conoscenza dei fatti, trattandosi di vicende direttamente connesse alla sfera di un personaggio pubblico protagonista nell'ambito della vita politica nazionale (candidato alle ultime elezioni politiche ed in lista, al momento della decisione sul ricorso da lui presentato, per le elezioni del Parlamento europeo), la richiesta di sottrarre le notizie alla reperibilità tramite

i motori di ricerca è stata respinta (*Provv.* 22 maggio 2009 [doc. *web* n. 1635938]).

I rischi legati all'uso della rete internet come fonte di informazioni e dati personali sono stati evidenziati dall'accoglimento di due segnalazioni con cui veniva lamentato che, a corredo della notizia del decesso di due persone, su alcuni giornali ed emittenti televisive erano state pubblicate fotografie acquisite direttamente da un noto *social network*, erroneamente attribuite, per pura omonimia, ai deceduti. In siffatte pubblicazioni l'Autorità ha riscontrato una violazione delle disposizioni a tutela del diritto alla protezione dei dati personali e dell'identità personale, poiché sono state raccolte informazioni non adeguatamente verificate e diffusi dati personali errati (*Provvedimenti* 6 maggio 2009 [doc. *web* nn. 1615317 e 1615339]).

1.1.5. Iniziativa economica - Profilazioni personalizzate e marketing *telefonico*

In materia di *marketing* alcune significative decisioni dell'Autorità sono state funzionali ad assicurare la correttezza del trattamento dei dati, in particolare con riferimento ad informativa e consenso dell'interessato.

Si è riferito in altra parte della presente *Relazione* (*par.* 1.1.2.) delle norme temporanee ovvero dell'art. 44, comma 1-*bis*, del d.l. 30 dicembre 2008, n. 207, convertito, con modificazioni, in l. 27 febbraio 2009, n. 14 che hanno consentito, in via derogatoria, fino al 31 dicembre 2009, per fini promozionali, l'utilizzo dei dati personali presenti nelle banche dati costituite sulla base dei vecchi elenchi telefonici precedentemente al 1° agosto 2005, nonché del *provvedimento* del Garante 12 marzo 2009 [doc. *web* n. 1598808] volto a precisare i limiti entro i quali le società che effettuano attività promozionale, anche tramite *call center*, possono avvalersi di tali disposizioni.

Al riguardo, tuttavia, è intervenuto l'art. 20-*bis* della l. 20 novembre 2009, n. 166 (in *G.U.* 24 novembre 2009, S.O. n. 215, con la quale è stato convertito, con modificazioni, il d.l. 25 settembre 2009, n. 135), che ha modificato l'art. 130 del Codice, consentendo il trattamento dei dati mediante l'impiego del telefono per finalità di invio del materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, nei confronti di chi non abbia esercitato il diritto

di opposizione mediante l'iscrizione della numerazione della quale è intestatario in un registro pubblico delle opposizioni, del quale ha previsto l'istituzione. Peraltro si evidenzia che, con *provvedimento* generale del 25 giugno 2009 [doc. *web* n. 1629107] sono state dettate le regole per il corretto uso dei dati personali a fini di profilazione nel settore delle telecomunicazioni, essendo emerso, anche a seguito di numerose ispezioni, che i gestori telefonici, senza il consenso degli interessati, avevano assai spesso usato i dati dei loro clienti, per profilare tra l'altro le abitudini, conoscere le preferenze, analizzare le spese telefoniche di tali soggetti.

Il Garante ha ribadito, innanzitutto, che i dati non possono essere utilizzati per le menzionate finalità senza un'adeguata informativa e senza l'esplicito consenso degli interessati.

Tuttavia rispetto ai dati trattati in forma "aggregata", è stato previsto che i gestori telefonici possano anche chiedere una specifica verifica preliminare, indicando le modalità del trattamento che intendono effettuare. Nell'ambito di tale verifica il Garante potrà valutare, caso per caso, se consentire tali trattamenti senza l'esplicito consenso degli interessati. Anche in questa ipotesi tuttavia dovrà essere data sempre una adeguata informativa ai clienti.

Ai gestori che già svolgono questa attività è stato dato il termine del 30 settembre 2009 per regolarizzare i trattamenti, e chiedere al Garante la necessaria verifica. Le suddette regole sono applicabili alle attività di profilazione avviate dopo l'entrata in vigore del *provvedimento.*

A seguito di numerose segnalazioni, inoltre, il Garante ha per la prima volta vietato l'effettuazione di telefonate commerciali tramite un sistema che generava i numeri da contattare attraverso sequenze casuali, elaborate con criteri geografici (*Provv.* 3 dicembre 2009 [doc. *web* n. 1679436]).

L'Autorità ha al riguardo chiarito che anche il numero casualmente composto e chiamato telefonicamente deve considerarsi *"dato personale"*, in quanto ricollegabile, anche indirettamente, a una persona identificata o identificabile. Sicché, per utilizzare anche questo tipo di numerazione a fini commerciali è necessario il previo consenso dell'interessato.

L'Autorità si è inoltre occupata della *cd.* "ricerca inversa", ossia della possibilità, per i fornitori di servizi di informazione sugli elenchi, di comunicare, *online* o al telefono, i dati personali degli abbonati, ricercati in base al numero telefonico o ad altra informazione personale.

In materia, il Garante aveva stabilito in particolare che l'attivazione della funzione di "ricerca inversa" presuppone il consenso specifico degli interessati (*cfr. Provv.* 15 luglio 2004 [doc. *web* n. 1032381], Allegato I, punto 4.2.1) da raccogliere tramite il questionario contenuto nel modulo di informativa e raccolta del consenso di cui all'Allegato IV del *provvedimento* ora citato.

Successivamente con numerose istanze, alcuni fornitori di servizi di informazione sugli elenchi avevano chiesto di modificare tale disciplina poiché, in assenza di risposta al detto questionario, i dati personali degli abbonati già presenti nei vecchi elenchi erano stati inseriti automaticamente anche nei nuovi elenchi, ma, non essendo in passato stata chiesta agli stessi alcuna manifestazione di volontà in merito all'utilizzabilità dei loro dati nei servizi di ricerca inversa, tale funzione, in assenza di risposta, era stata generalmente intesa come inibita nei loro confronti.

Alla luce di ciò l'Autorità, con *provvedimento* 8 aprile 2010 successivamente pubblicato nella *Gazzetta Ufficiale* [doc. *web* n. 1713429] in un'ottica di semplificazione, ha disposto che, con esclusivo riferimento ai "vecchi" abbonati i cui dati erano già inseriti in un elenco pubblico alla data del 1° febbraio 2005, possa essere attivata a partire dal 1° gennaio 2011 - previa idonea informativa nella bolletta telefonica entro il 31 dicembre 2010 e sui siti *web* dei gestori entro il 31 maggio 2010 - la funzione di ricerca inversa anche senza il consenso espresso degli abbonati, salvo il rispetto di eventuali volontà contrarie comunicate dagli stessi al proprio operatore.

Di rilievo generale anche la decisione (*Provv.* 1° aprile 2010, successivamente pubblicato sulla *Gazzetta Ufficiale* [doc. *web* n. 1711492]) riguardante il *database* unico (Dbu) utilizzato per formare gli elenchi telefonici, basati su dati inseriti dai singoli operatori di telefonia in base al consenso espresso dai clienti (*cfr.* delibera Agcom 6 febbraio 2002, n. 36/02/CONS).

Gli operatori del settore, segnalando un significativo decremento delle utenze presenti nel Dbu in un arco di tempo relativamente breve, hanno ricondotto il fenomeno alla mancata compilazione, da parte dei clienti che cambiano operatore telefonico, del modulo per esprimere il consenso all'inserimento nel Dbu (di cui all'Allegato IV del *cit. provvedimento* 15 luglio 2004).

Al riguardo, nella *decisione* dell'aprile 2010 si è ricordato che, anche se l'interessato decide di conservare il numero telefonico - *number portability* (*Np*) - in caso di attivazione di una nuova utenza telefonica, anche mobile, il nuovo operatore è tenuto a sottoporgli il modulo di informativa e raccolta del consenso.

Tuttavia, poiché il numero telefonico non cambia e, quindi, restano invariati tutti gli elementi oggetto di pubblicazione negli elenchi, il Garante ha ritenuto che i clienti che modificano l'operatore con *Np* possano essere assimilati ai "vecchi" clienti di cui al *provvedimento* del 2004, ossia a quei soggetti i cui nominativi erano già presenti negli elenchi pubblicati prima dell'entrata in vigore del nuovo regime degli elenchi telefonici. Anche i predetti soggetti infatti hanno già espresso in passato al proprio operatore la volontà di inserimento nel Dbu e, conseguentemente, negli elenchi, dei dati personali che li riguardano.

Pertanto, per tale categoria di utenti, il nuovo operatore telefonico può mantenere invariate le opzioni scelte in passato, in assenza di risposta al questionario entro sessanta giorni dalla ricezione dello stesso, fermo restando che gli interessati possono manifestare in qualunque momento, al nuovo operatore, una diversa volontà.

1.1.6. Attività d'impresa

Il trattamento di dati all'interno dell'impresa o dei gruppi di impresa è stato oggetto nel 2009 di deliberazioni del Garante di rilievo generale.

Con *deliberazione* del 10 dicembre 2009 [doc. *web* n. 1693019] l'Autorità ha deciso di segnalare a Parlamento e Governo l'opportunità di un intervento normativo per disciplinare (in sintonia con il parere 1° febbraio 2006 del Gruppo Art. 29), i sistemi di segnalazione (*cd. "whistleblowing"*) di illeciti commessi da soggetti operanti a vario

titolo nell'organizzazione aziendale, nonché i profili di interferenza di tale fenomeno con la disciplina di protezione dei dati. Occorre al riguardo segnalare che altri ordinamenti, quali quello degli Stati Uniti e della Gran Bretagna, hanno già adottato provvedimenti legislativi in merito, prevedendo, tra l'altro, misure a protezione degli autori (in buona fede) delle segnalazioni.

L'Autorità ha evidenziato che manca nel nostro ordinamento una disciplina di carattere generale sulla liceità del trattamento di dati nell'ambito di tali sistemi di segnalazione, che pure potrebbero tutelare anche interessi di carattere generale "esterni" all'azienda, (*ad es.*, tutela della stabilità dei mercati finanziari, lotta alla corruzione, contrasto alla criminalità economica e finanziaria, tutela dei risparmiatori). Appaiono da disciplinare, con norma primaria, in particolare i profili relativi: all'individuazione dei soggetti operanti all'interno delle società che possono assumere la qualità di segnalanti, delle finalità che si intendono perseguire, delle fattispecie oggetto di possibile "denuncia" da parte dei segnalanti. Occorre chiarire la portata del diritto di accesso previsto dall'art. 7 del Codice da parte del soggetto al quale si riferisce la segnalazione (interessato), con riguardo ai dati identificativi dell'autore della segnalazione (denunciante), nonché l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

Con *deliberazione* 10 settembre 2009 (in *G.U.* 16 novembre 2009, n. 267 [doc. *web* n. 1664492]) l'Autorità ha affrontato la questione del coordinamento tra la normativa di protezione dei dati personali e la disciplina di settore in materia di antiriciclaggio (in ordine alla quale il Garante si era espresso con il *parere* del 25 luglio 2007 [doc. *web* n. 1431012]).

In proposito l'Autorità, ponderando gli interessi in gioco, ha deciso che i titolari del trattamento tenuti ad effettuare una segnalazione antiriciclaggio in conformità alla disciplina di settore (d.lgs. n. 231/2007) possono dare comunicazione dell'avvenuta segnalazione agli intermediari finanziari appartenenti al medesimo gruppo, senza che a tal fine sia necessario acquisire il consenso degli interessati (art. 24, comma 1, lett. *g*) del Codice). Inoltre, ai titolari del trattamento è stato prescritto (ai sensi degli artt. 143, comma 1, lett. *b*), e 154, comma 1, lett. *c*), del Codice) di fornire agli interessati

specifiche indicazioni anche sulla possibilità che le informazioni relative alle operazioni poste in essere dagli stessi interessati, ove queste siano ritenute "sospette" ai sensi dell'art. 41, comma 1, del d.lgs. 21 novembre 2007, n. 231, siano comunicate ad altri intermediari finanziari appartenenti al medesimo gruppo.

A seguito di richieste riguardanti operazioni di riassetto nel settore bancario, relative ad un numero estremamente elevato di soggetti interessati, il Garante ha individuato le modifiche che, nelle operazioni societarie di fusione o scissione, devono essere fornite rispetto all'informativa resa in precedenza dalla società scissa o dalle società partecipanti alla fusione (art. 154, comma 1, lett. *c*) e *h*), del Codice) (*Provv.* 8 aprile 2009 [doc. *web* n. 1609999]).

In sostanza, ha previsto che le società coinvolte nel processo di fusione o scissione informino tutti i soggetti interessati (clienti, lavoratori, fornitori, *ecc.*) su chi sia il titolare e il nuovo responsabile del trattamento dei dati personali in possesso dell'impresa, al quale potersi rivolgere per esercitare il diritto di accesso e tutti gli altri diritti previsti dal Codice.

Per semplificare gli adempimenti, l'Autorità ha deciso che in un primo tempo potrà essere fornita una comunicazione generale immediata, sui siti *web* delle società coinvolte, non appena definito il nuovo assetto societario. Alla prima occasione di contatto, poi, le società dovranno comunque inviare i nuovi riferimenti a tutti gli interessati.

Nel caso in cui le società risultanti dal processo di fusione o scissione effettuino trattamenti in cui è prevista la notificazione al Garante, tali aziende dovranno effettuare o integrare la notificazione secondo le procedure *standard* già previste dall'Autorità.

Con *deliberazioni* del 18 marzo 2010, nn. 18 e 19 [doc. *web* nn. 1708078 e 1709118] è stato determinato il contributo spese che i Sistemi di informazione creditizie (Sic) gestiti da Crif S.p.A., nonché *Experian information services*, Cts e Assilea, potranno richiedere - in qualità di titolari presso i quali *"si determina un notevole impiego di mezzi in relazione ... all'entità delle richieste"* - agli interessati in caso di esercizio dei diritti ai sensi dell'art. 7, commi 1 e 2, lett. *a*), *b*), *c*), del Codice, secondo quanto previsto dall'art. 10, commi 7 e 8, 1° cpv., del Codice, e in ottemperanza a quanto disposto dal Consiglio di Stato con sentenza n. 5198/09.

Nel merito è stato deciso, tra l'altro, che: tutte le volte in cui l'interessato richieda espressamente il riscontro attraverso l'invio a mezzo di posta elettronica, lo stesso dovrà essere reso a titolo gratuito; per le richieste successive alla prima, nell'arco di ciascun anno solare, formulate ai sensi dell' art. 7, commi 1 e 2, lett. *a*) e *b*), potrà essere richiesto un contributo spese commisurato ai costi effettivamente sostenuti e, comunque, non superiore a 7 euro (incluse le spese postali); qualora sia presentata una richiesta incompleta e per fornire un idoneo riscontro si renda indispensabile contattare l'interessato, il contributo spese non dovrà superare i costi effettivamente sostenuti e, in ogni caso, l'importo di 3 euro.

1.1.7. Protezione dei dati dei lavoratori dipendenti e dei collaboratori

Alcuni provvedimenti adottati dal Garante nel 2009 sul trattamento dei dati personali in ambito lavoristico - con particolare riferimento ai dati sulla salute dei dipendenti - evidenziano la duplice esigenza di rispettare i princìpi di pertinenza e non eccedenza dei dati trattati e di evitare improprie forme di circolazione delle informazioni, all'esterno, ma anche all'interno dell'ambito lavorativo.

Al riguardo, si cita il *provvedimento* con il quale il Garante ha intimato alla Provincia di Foggia il blocco dei dati sulla salute di una dipendente, la quale aveva segnalato la diffusione - attraverso il sito internet del menzionato ente locale presso il quale lavorava, nonché attraverso il motore di ricerca *Google* - di due determinazioni riguardanti la propria richiesta di riconoscimento dell'infermità da causa di servizio (*Provv.* 25 giugno 2009 [doc. *web* n. 1640102]). Uno dei documenti riportava, in particolare, accanto al nome e cognome della dipendente, la valutazione medico-legale relativa al tipo di infermità riscontrata, in violazione del divieto di diffusione di dati relativi alla salute (art. 2, comma 7, d.P.R. 29 ottobre 2001, n. 461 e tab. A, allegata al d.P.R. 30 dicembre 1981, n. 834; *v.* anche art. 6 decreto 12 febbraio 2004).

Con *provvedimento* 24 settembre 2009 [doc. *web* n. 1658058] è stato altresì disposto il blocco, nei confronti di una commissione medica di verifica del Ministero dell'economia e delle finanze, dei dati sensibili contenuti in un verbale di accertamento

di inidoneità all'impiego di un'insegnante. L'organo di accertamento aveva trasmesso copia integrale del verbale di visita; l'Autorità ha richiesto alla commissione medica di utilizzare un attestato riportante la sola valutazione medico-legale ai fini della comunicazione, alle amministrazioni di appartenenza dei lavoratori, dell'esito degli accertamenti sanitari di inidoneità al servizio o altre forme di inabilità non dipendenti da causa di servizio.

È stato ritenuto illecito anche il trattamento dei dati sanitari della docente posto in essere dall'amministrazione scolastica presso cui prestava servizio, in ragione dell'inutilizzabilità delle informazioni trattate in violazione della disciplina sulla protezione dei dati (artt. 11 e 22, commi 1, 3 e 5, del Codice; art. 5, l. n. 135/1990; artt. 4, 5 e 6, comma 8, d.P.R. n. 461/2001; *v.* anche punti 3.2 e 8.4 delle *"Linee-guida sul trattamento di dati dei lavoratori per la gestione del rapporto di lavoro in ambito pubblico"* (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]). L'amministrazione avrebbe dovuto limitarsi ad utilizzare la valutazione medico-legale, adottando ogni misura per l'ulteriore conservazione del documento idonea a limitarne rigorosamente la conoscibilità.

Con *provvedimento* 21 ottobre 2009 [doc. *web* n. 1689440] è stata ritenuta fondata la segnalazione di un militare cessato dal servizio per permanente inidoneità, il quale aveva contestato la liceità del trattamento dei suoi dati personali detenuti dall'ufficio del personale del Ministero della difesa, rappresentando che questo, avente competenze non sanitarie in materia di stato giuridico, avanzamento e contenzioso del personale militare, avesse indebitamente raccolto informazioni relative al suo stato di salute attraverso l'acquisizione di certificazioni e verbali di visita medica formati dagli organismi militari.

Nella specie, la documentazione medica trasmessa dalle commissioni mediche militari all'ufficio del personale era risultata contenere informazioni non necessarie per l'adozione dei provvedimenti di competenza in materia di stato giuridico e di avanzamento dei militari. Richiamando le indicazioni fornite nelle linee-guida in materia di trattamento di dati personali dei dipendenti pubblici, il Garante ha pertanto richiesto all'amministrazione di rendere conformi alla normativa sulla riservatezza le modalità di circolazione interna dei dati sulla salute del personale.

Nello stesso senso la *decisione* (2 ottobre 2009 [doc. *web* n. 1658119]), che ha ritenuto

fondato il reclamo con cui un dipendente aveva contestato l'indicazione del suo nome e della diagnosi, nel verbale della visita collegiale, trasmesso dalla commissione medica all'Ispettorato di sanità della marina militare, ai fini dell'attestazione dell'idoneità al servizio. La copia del verbale inviata all'ufficio del personale con la diagnosi *"sbarrata e omessa"* consentiva, seppur indirettamente, di risalire all'infezione Hiv, essendo questa l'unica patologia per la quale è prevista la "cancellazione" dai verbali di accertamento medico.

Ribadito che ai dipendenti sieropositivi deve essere assicurata garanzia assoluta di anonimato, il Garante, oltre a inibire l'uso dei dati del dipendente, ha ordinato al Ministero di conformare alla normativa sulla riservatezza la circolazione dei dati sanitari al suo interno e di informare i lavoratori chiaramente sull'obbligatorietà o meno di fornire dati sulla propria salute e sulle relative conseguenze nell'ambito degli accertamenti medico-legali ai fini dell'idoneità al servizio.

Si segnala infine il *provvedimento* 4 marzo 2010 [doc. *web* n. 1706464] con cui il Garante ha espresso parere favorevole in ordine a 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, predisposto in attuazione delle linee-guida adottate dal Garante il 1° marzo 2007, in merito all'uso di internet e della posta elettronica sul luogo di lavoro.

1.1.8. Dati genetici e sanitari

Nel quadro del processo di ammodernamento della sanità pubblica e privata, dopo un'articolata procedura di consultazione pubblica (*cfr. Relazione 2008*, p. 17 e *Deliberazione* n. 8 del 5 marzo 2009, in *G.U.* 26 marzo 2009, n. 71 [doc. *web* n. 1598313]), e tenuto conto delle osservazioni formulate dal gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali sono state adottate, in attesa di un'adeguata legislazione in materia, le *"Linee-guida in tema di fascicolo sanitario elettronico (Fse) e di* dossier *sanitario"* (*Provv.* 16 luglio 2009, *G.U.* 3 agosto 2009, n. 178 [doc. *web* n. 1634116]).

Il *provvedimento* stabilisce, in particolare che il paziente deve poter scegliere, in piena libertà, se far costituire o meno un fascicolo sanitario elettronico, con tutte o solo alcune delle informazioni sanitarie che lo riguardano; deve poter manifestare un consenso autonomo e specifico, distinto da quello che si presta a fini di cura della salute; al paziente deve essere inoltre garantita la possibilità di *"oscurare"* la visibilità di alcuni eventi clinici, così come, in generale, egli può decidere di non informare il medico di alcuni eventi sanitari che lo riguardano. Un consenso specifico è richiesto per informazioni particolarmente delicate, quali quelle relative ad atti di violenza sessuale, pedofilia, allo stato di sieropositività, all'interruzione volontaria di gravidanza.

L'informativa, in termini chiari e dettagliati, deve indicare chi (medici di base, del reparto ove è ricoverato il paziente, farmacisti) ha accesso ai dati e che tipo di operazioni può compiere.

Il fascicolo sanitario elettronico potrà essere consultato dal paziente con modalità adeguate (*ad es.*, tramite *smart card*) e dal personale sanitario strettamente autorizzato, solo per finalità sanitarie, non invece da periti, compagnie di assicurazione, datori di lavoro.

Il paziente che non vuole aderire al Fse deve poter usufruire comunque delle prestazioni del Servizio sanitario nazionale.

Per garantire la sicurezza del trattamento gli accessi alle informazioni dovranno essere tracciabili e graduali e i dati sanitari dovranno essere protetti con misure di sicurezza che limitino il più possibile i rischi di abusi, furti e smarrimento.

Dopo una consultazione pubblica (avviata con *Deliberazione* 25 giugno 2009 [doc. *web* n. 1630271]), grazie alla quale sono state raccolte osservazioni formulate da professionisti sanitari, organismi rappresentativi ed associazioni di pazienti il Garante, con *provvedimento* 19 novembre 2009 [doc. *web* n. 1679033], ha altresì approvato le *"Linee-guida in tema di referti* online", che fissano rigorose misure a protezione dei dati sanitari dei pazienti che ricevono il referto via mail o "scaricano" gli esami clinici direttamente dal sito *web* della struttura sanitaria.

Anche in questo caso, come per il fascicolo sanitario elettronico, l'Autorità ha sostanzialmente svolto un ruolo di supplenza in attesa dell'adozione di una apposita normativa.

In sintesi, nel menzionato *provvedimento* è previsto che l'adesione al servizio sia facoltativa e che il referto elettronico non sostituisca quello cartaceo, che rimarrà comunque disponibile. Per chiedere il consenso dell'assistito occorre fornire una informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di *"refertazione online"*.

Il referto resterà a disposizione *online* per un massimo di quarantacinque giorni e dovrà essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato.

Le strutture sanitarie dovranno adottare importanti misure di sicurezza tecnologica (utilizzo di *standard* crittografici, sistemi di autenticazione "forte" convalida degli indirizzi e-mail con verifica *online*, uso di *password* per l'apertura del *file*) e, per offrire la possibilità di archiviare e continuare a consultare via *web* i referti, acquisire un autonomo consenso sulla base di un'ulteriore specifica informativa.

A conclusione dell'attività istruttoria, di cui si è riferito nella *Relazione 2008* (*cfr.* p. 75), è emerso che il controllo a fini tributari della natura e della qualità dei farmaci venduti, richiesto dalla legge, può essere effettuato attraverso l'utilizzo del "numero di autorizzazione all'immissione in commercio" (Aic) presente sulla confezione dei farmaci. Il codice alfanumerico, rilevabile anche mediante lettura ottica, consente, infatti, di identificare in modo univoco ogni singola confezione farmaceutica venduta.

Nel rispetto della normativa vigente, pertanto, il Garante ha prescritto che, a partire dal 1° gennaio 2010, lo scontrino fiscale rilasciato dalle farmacie per dedurre e detrarre la spesa sanitaria nella dichiarazione dei redditi riporti, in luogo dello specifico nome del farmaco acquistato, l'indicazione del codice alfanumerico posto sulla confezione di ogni medicinale (*Provv.* 29 aprile 2009 [doc. *web* n. 1611565]).

Nella *Relazione 2008*, p. 96, si è dato conto dell'avvio del processo di revisione dell'*autorizzazione* generale al trattamento dei dati genetici (*Provv.* 22 febbraio 2007 [doc. *web* n. 1389918]). All'esito della menzionata revisione il Garante, in data 12 dicembre 2009, ha approvato in via preliminare, ed inviato al Ministro della salute per il parere del Consiglio superiore di sanità, un nuovo schema di autorizzazione, che tiene conto dell'esperienza maturata e delle osservazioni di qualificati esperti,

con particolare riferimento all'aggiornamento delle definizioni utilizzate, ai trattamenti effettuati per la tutela della salute di familiari in assenza del consenso dell'interessato, alle ricerche scientifiche che coinvolgono soggetti vulnerabili senza comportare per loro alcun beneficio diretto, nonché alla comunicazione ai familiari dell'interessato di dati genetici indispensabili per evitare un grave pregiudizio per la loro salute.

In attesa della definizione della predetta procedura consultiva, l'efficacia della vigente *autorizzazione* generale è stata prorogata al 30 aprile 2010 (*Provv.* 22 dicembre 2009 [doc. *web* n. 1683067]) e potrà esserlo ulteriormente qualora l'*iter* previsto non si perfezioni nel frattempo.

Con un *provvedimento* generale del 12 novembre 2009 [doc. *web* n. 1686068], essendo emerso che diversi studi medici e dentistici raccoglievano informazioni sull'Hiv mediante la distribuzione di un questionario al momento dell'accettazione dei pazienti, sono stati indicati i princìpi ai quali devono attenersi i medici nella raccolta di informazioni sulla sieropositività.

In sintesi, l'Autorità ha stabilito che gli esercenti la professione sanitaria non possono raccogliere informazioni sulla sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, se ciò non è indispensabile per il tipo di intervento o terapia da eseguire, e comunque è al riguardo necessario il consenso dell'interessato. La raccolta di informazioni sull'Hiv fin dall'accettazione non può essere giustificata neanche dalla necessità di attivare specifiche misure di protezione per il contagio, che la normativa di settore prevede siano adottate nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività. Infine, il medico che venga a conoscenza di un caso di Aids o di Hiv, oltre a rispettare specifici obblighi di segretezza e non discriminazione nei confronti del paziente, ha l'obbligo di adottare ogni misura individuata dal Codice per garantire la sicurezza dei dati sanitari.

Appare di interesse anche la *decisione*, adottata a seguito di ricorso, del 17 settembre 2009 [doc. *web* n. 1656642] relativa alla richiesta del convivente superstite di accedere alle informazioni contenute nella cartella clinica e nei referti diagnostici detenuti dalla struttura ospedaliera nella quale la *de cuius* era stata ricoverata ed era poi deceduta.

La richiesta è stata accolta, atteso che il convivente ha esercitato il diritto per disporre delle informazioni necessarie ad intraprendere le azioni giudiziarie volte a verificare eventuali inadempienze nelle prestazioni sanitarie rese dalla struttura ospedaliera.

La tematica del consenso è stata oggetto specifico dell'*autorizzazione* (*Provv.* 16 aprile 2009 [doc. *web* n. 1611936]) rilasciata ad un istituto di ricovero e cura a carattere scientifico per condurre, su circa ventimila pazienti affetti da patologie neoplastiche mammarie, uno studio epidemiologico retrospettivo volto all'individuazione del miglior trattamento del carcinoma mammario operabile.

Dall'istruttoria è emerso che lo studio, di durata limitata, non avrebbe potuto raggiungere i suoi scopi senza l'identificazione, anche temporanea, degli interessati e che il trattamento era limitato ai soli dati personali contenuti nelle cartelle cliniche di pazienti curati in precedenza dallo stesso istituto e conservate da questi a norma di legge. Ancora, l'istituto si era impegnato a raccogliere le manifestazioni di volontà di quegli assistiti che si sarebbero nuovamente recati presso la struttura per il *follow-up* e a non comunicare in alcun modo o diffondere le informazioni utilizzate per la ricerca.

L'iniziativa è stata autorizzata, anche in assenza del consenso informato dei pazienti, in ragione dello scopo scientifico perseguito, delle specifiche modalità di trattamento previste, nonché della limitata durata temporale dello studio, anche alla luce del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (art. 11, [doc. *web* n. 1038384]).

Nella *Relazione 2006*, p. 62, si è riferito del divieto di pubblicare, sul sito internet di una regione, le graduatorie per la concessione di contributi regionali indicanti, tra l'altro, le generalità e le motivazioni di esclusione dalle stesse di circa quattromilacinquecento soggetti disabili (*Provv.* 18 gennaio 2007 [doc. *web* n. 1382026]).

A seguito di una segnalazione l'Autorità, accertato che le suddette graduatorie, rimosse solo da alcune pagine, erano ancora presenti sul sito, ha vietato alla regione (*Provv.* 17 settembre 2009 [doc. *web* n. 1658335]) la diffusione, in particolare tramite il sito istituzionale, dei dati idonei a rivelare lo stato di salute degli interessati contenuti nei documenti relativi agli elenchi e alle graduatorie dei disabili.

Si segnala anche che il Garante, il 16 dicembre 2009 [doc. *web* n. 1689676] ha espresso *parere* favorevole, con osservazioni, in ordine a uno schema di disegno di legge governativo recante l'istituzione del registro nazionale e dei registri regionali degli impianti protesici mammari. L'Autorità, pur dichiarando di condividere le linee generali del disegno di legge e le finalità perseguite, ne ha tuttavia evidenziato talune criticità segnatamente sotto i profili dell'individuazione delle specifiche finalità perseguite con l'istituzione dei registri, delle categorie di dati oggetto di trattamento, nonché del regime di conoscibilità dei dati conservati nei registri ed ha suggerito al Governo l'adozione di misure idonee a soddisfare tali esigenze.

Si ricorda infine che in data 21 gennaio 2010 il Garante ha espresso *parere* favorevole [doc. *web* n. 1693904], con osservazioni volte ad evitare l'utilizzo di informazioni non indispensabili, in ordine a uno schema di decreto del Ministro per la pubblica amministrazione e l'innovazione, relativo alle modalità di assorbimento della tessera sanitaria nella carta nazionale dei servizi, cosicché le regioni possano distribuire un'unica *smart card* che assolva ad entrambe le funzioni e consenta l'accesso ai servizi erogati in rete, nel rispetto degli *standard* di sicurezza previsti dal Codice.

1.1.9. Videosorveglianza e biometria

Videosorveglianza

In materia di videosorveglianza si segnalano, da un lato, alcuni significativi provvedimenti diretti ad assicurare il rispetto del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482], dall'altro, il provvedimento sulle nuove linee-guida.

Sul primo punto, si era rivolta all'Autorità la Soprintendenza speciale per il polo museale napoletano, alla quale il Comando dei Carabinieri-tutela patrimonio culturale nucleo di Napoli aveva chiesto di conservare per almeno trenta giorni le immagini raccolte tramite i sistemi di videosorveglianza installati presso alcuni musei della Regione Campania, maggiormente esposti al rischio della minaccia terroristica.

Per l'eccezionalità della situazione prospettata, considerato che la normativa di settore consente controlli continuativi tramite impianti audiovisivi per garantire la sicurezza dei beni culturali esposti o comunque raccolti e depositati nei musei statali

(art. 1, d.l. 14 novembre 1992, n. 433) e richiamando l'esigenza di rispettare i princìpi generali di liceità, necessità, proporzionalità e finalità affermati dal Codice (artt. 3, 11, comma 1, lett. *a*) e *d*) e 18, comma 2, del Codice e punto 2.1. del *provvedimento* aprile 2004), il Garante ha prescritto alla Soprintendenza, con *provvedimento* adottato ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, di conservare le immagini raccolte presso alcuni siti museali della Regione Campania per un periodo di trenta giorni, fintantoché persiste la dichiarata eccezionale necessità (*Provv.* 12 marzo 2009 [doc. *web* n. 1605521]).

È altresì da menzionare l'approvazione (condizionata), in sede di verifica preliminare (art. 17 del Codice), di un apparato di videosorveglianza presso un istituto scolastico di Verona a salvaguardia del patrimonio scolastico, contro teppismo ed atti vandalici (*Provv.* 4 settembre 2009 [doc. *web* n. 1651744]).

In conformità al suddetto *provvedimento* del 2004, è stata prevista l'attivazione delle telecamere solo negli orari di chiusura degli istituti. Tuttavia, nel caso in cui l'attività didattica o ad essa strumentale all'interno della scuola coincida con l'orario di attivazione delle telecamere, è stata ritenuta necessaria la definizione, in accordo con il dirigente scolastico, degli orari di funzionamento delle telecamere.

Le telecamere possono riprendere esclusivamente le mura esterne, devono essere segnalate da appositi cartelli con visibilità anche notturna e la visualizzazione delle immagini è stata consentita solo a polizia e autorità giudiziaria.

Biometria

Sempre in sede di verifica preliminare (*Provv.* del 17 settembre 2009 [doc. *web* n. 1655708]), una società che svolge attività di vigilanza e sicurezza è stata autorizzata a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa. Nel progetto sottoposto alla verifica era previsto che i dati biometrici dei dipendenti, costituiti da caratteristiche tratte dall'impronta digitale, fossero memorizzati sotto forma di *template* ed in modalità cifrata, su un supporto (*smart card*) posto nell'esclusiva disponibilità del lavoratore. Il progetto escludeva comunque il controllo sull'orario di lavoro.

L'Autorità ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei dipendenti in relazione agli accessi alle sole *"aree sterili"*, prescrivendo tuttavia

alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa sulla natura facoltativa del consenso al trattamento dei dati biometrici. La conservazione dei dati relativi agli accessi alle *"aree sterili"* è stata approvata per un tempo massimo di sette giorni.

Il nuovo provvedimento in materia di videosorveglianza

Anche in base al nuovo *provvedimento* generale dell'8 aprile 2010 in materia di videosorveglianza ([doc. *web* n. 1712680], in pubblicazione in *G.U.*), adottato previa consultazione del Ministero dell'interno, dell'Associazione nazionale comuni italiani e dell'Unione delle province d'Italia, l'Autorità ha ribadito, tra l'altro, che devono essere utilizzati solo dati anonimi quando le finalità del trattamento lo consentono e comunque unicamente immagini pertinenti e non eccedenti rispetto alle finalità perseguite.

Gli interessati devono essere resi edotti dell'esistenza di sistemi di videosorveglianza, anche attraverso il modello di informativa "minima" messo a disposizione nel *provvedimento* del 2004 *cit.* (art. 13, comma 3, del Codice). È stato, altresì, predisposto un nuovo modello semplificato per i titolari del trattamento che intendono attivare un collegamento diretto con le forze di polizia.

I sistemi che associano immagini a dati biometrici e quelli capaci di rilevare automaticamente comportamenti o eventi anomali e segnalarli devono essere sottoposti alla verifica preliminare, poiché comportano rischi specifici per i diritti e le libertà fondamentali.

Per quanto riguarda le misure di sicurezza l'Autorità ha disposto, tra l'altro, che: agli incaricati e responsabili del trattamento devono essere conferiti diversi livelli di visibilità e trattamento delle immagini, in relazione alle diverse competenze di ciascuno; occorre limitare le ipotesi di visione delle immagini raccolte e registrate e predisporre specifiche misure per la cancellazione delle immagini conservate nonché applicare tecniche crittografiche per la trasmissione di immagini da una rete pubblica o tramite connessioni *wireless.*

Fatte salve speciali esigenze di ulteriore conservazione in relazione alla chiusura di uffici o esercizi, o specifiche richieste a scopo investigativo delle autorità preposte, le immagini devono essere conservate al massimo per ventiquattro ore, dopo la loro rilevazione e solo per peculiari esigenze tecniche o per la particolare rischiosità

dell'attività del titolare del trattamento sino a una settimana.

Per i comuni, e solo per fini di tutela della sicurezza urbana, il termine massimo è di sette giorni, salvo eccezionali esigenze da sottoporre a una verifica preliminare del Garante.

L'informativa agli interessati è necessaria anche nei casi in cui i sindaci, quali ufficiali del Governo, o i comuni utilizzano sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutelare la sicurezza urbana.

La rilevazione di immagini tramite sistemi di videosorveglianza svolta da soggetti privati può avere legittimamente luogo previa acquisizione del consenso degli interessati o in presenza di un requisito equipollente (artt. 23 e 24 del Codice). A tal proposito, il provvedimento ha individuato i casi in cui, per la tutela di persone o di beni, la rilevazione di immagini può avvenire senza la previa acquisizione del consenso.

Per i *cd. "sistemi integrati di videosorveglianza"* tra soggetti diversi sono state previste specifiche garanzie per quei trattamenti che sono effettuati mediante: l'utilizzo, da parte di diversi e autonomi titolari del trattamento, delle stesse infrastrutture tecnologiche; il collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; il collegamento con le forze di polizia, anche nelle predette ipotesi.

Al riguardo, sono state prescritte alcune misure di sicurezza ulteriori quali l'adozione di sistemi per la registrazione degli accessi logici e delle operazioni compiute sulle immagini registrate e la separazione logica delle immagini registrate dai diversi titolari.

Con specifico riferimento ai sistemi di videosorveglianza integrati utilizzati dagli enti territoriali, inoltre, è stato stabilito che non possono essere tracciati gli spostamenti degli interessati e le immagini gestite da un unico centro devono essere trattate in forma differenziata.

Devono altresì essere sottoposti a verifica preliminare i sistemi integrati di videosorveglianza non rientranti nei modelli sopra descritti e per i quali non sia possibile adottare le misure e gli accorgimenti indicati nel provvedimento.

In considerazione del fatto che anche i dispositivi elettronici per la rilevazione di violazioni al codice della strada comportano un trattamento di dati personali, nel

circoscrivere le ipotesi di rilevazioni di immagini ai casi di infrazione, sono stati disciplinati il regime di accessibilità alle immagini rilevate ed i relativi tempi di conservazione, prevedendo, altresì, specifiche cautele per la riservatezza di eventuali passeggeri presenti a bordo dei veicoli.

Per l'adeguamento dei sistemi di videosorveglianza alle prescrizioni del *provvedimento*, sono stati infine indicati specifici termini, il cui mancato rispetto può comportare l'applicazione di una sanzione amministrativa.

1.1.10. Disposizioni relative agli eventi sismici verificatisi nella Regione Abruzzo

Per il terremoto dell'Aquila, tenuto conto della situazione di grave emergenza creatasi, il Garante ha sospeso nelle zone interessate, sino al 31 dicembre 2009, il decorso dei termini di adempimento di ogni provvedimento adottato dall'Autorità in materia di trattamento di dati personali, ai sensi dell'art. 154 del Codice (*Provv.* 28 maggio 2009, in *G.U.* 15 giugno 2009, n. 136 [doc. *web* n. 1620165]).

Inoltre, l'Autorità è stata interpellata dal Comune dell'Aquila circa le richieste delle forze politiche di acquisire per la campagna elettorale gli elenchi in cui, a seguito del sisma del 2009, sono registrati i nuovi recapiti degli elettori. Essi, privi dei riferimenti telefonici, sono stati raccolti dal Comune in apposite banche dati, correlate alle diverse tipologie di *"modalità abitative"* (quali moduli abitativi provvisori, moduli abitativi rimovibili, autonoma sistemazione all'interno e al di fuori del territorio aquilano), per controllare il movimento migratorio.

Al riguardo, in relazione ai soli profili di competenza del Garante, non è stata ritenuta preclusa, con riferimento alle specifiche esigenze rappresentate con il quesito, la possibilità che, per l'inoltro di messaggi elettorali e politici, possano essere forniti, ai richiedenti legittimati, gli indirizzi provvisori dei soli cittadini iscritti nelle liste elettorali in possesso del Comune dell'Aquila, con esclusione di ogni altra informazione non pertinente (*Provv.* 4 febbraio 2010 [doc. *web* n. 1694777]).

1.2. RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI

1.2.1. Le audizioni del Garante in Parlamento

Nel 2009 il Garante ha partecipato ad alcune audizioni presso commissioni della Camera e del Senato o altri organismi anche bicamerali, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di proposte di legge aventi riflessi in materia di protezione dei dati personali.

In questo quadro si collocano, in particolare:

a) il 25 novembre 2009, presso la Commissione finanze della Camera dei deputati, un'audizione nell'ambito dell'indagine conoscitiva sul credito al consumo, il cui documento conclusivo è stato approvato il 23 febbraio 2010. Nel corso dell'audizione il Garante ha affrontato diverse problematiche relative al funzionamento dei Sistemi di informazione creditizia (Sic) e all'applicazione del relativo codice di deontologia e buona condotta; si è poi soffermato anche sul progetto di legge in materia di furto d'identità e di frodi *"nel settore del credito al consumo e dei pagamenti dilazionati o differiti e del settore assicurativo"*, approvato dal Senato e successivamente assegnato all'esame proprio della Commissione finanze (AC 2699). Sul punto l'Autorità ha ribadito alcune perplessità già espresse nel corso di una audizione tenuta presso l'omologa Commissione del Senato il 31 luglio 2008, in particolare per quanto riguarda la paventata costituzione di una nuova banca dati, l'ampliamento della categoria dei dati acquisiti al fine di prevenire le frodi configuranti furto di identità e dei soggetti aderenti al sistema antifrode, nonché la previsione di una sua estensione anche alle frodi nel settore assicurativo; fenomeno, quest'ultimo, affatto diverso da quello relativo al furto d'identità oggetto del disegno di legge. Si segnala peraltro che il suddetto documento conclusivo mette in ampio risalto le osservazioni rese dal Garante nell'audizione sia per quanto riguarda i Sic, sia in relazione alle criticità evidenziate sul citato progetto di legge in materia di furto di identità e frodi nel settore del credito al consumo. Nel documento conclusivo si approfondisce in particolare la tematica relativa alle proposte di riforma, anche normativa, in materia, segnatamente per quanto riguarda:

- il rafforzamento dei poteri, anche sanzionatori, delle autorità di vigilanza;
- l'operatività dei Sic e gli strumenti a garanzia dei consumatori (informativa, opposizione, tutela);
- il potenziamento della capacità degli operatori del credito di effettuare un'autonoma valutazione del credito stesso;
- la necessità di una normativa specifica sul sovraindebitamento delle famiglie;
- la necessità di una normativa per combattere le frodi, con particolare riguardo al furto d'identità;

b) il 15 luglio 2009, presso la Commissione affari costituzionali della Camera, un'audizione nell'ambito dell'indagine conoscitiva sull'informatizzazione delle pubbliche amministrazioni (il cui documento conclusivo è stato approvato il 16 dicembre 2009), nel corso della quale il Garante ha in particolare illustrato le implicazioni sulla protezione dei dati personali dei processi di informatizzazione dell'attività amministrativa, specie per quanto riguarda l'uso della rete per la trasmissione, l'archiviazione e lo scambio di dati tra le strutture sanitarie nonché, talora, tra esse, medici curanti e pazienti. L'Autorità ha inoltre descritto i riflessi sul diritto alla protezione dei dati personali derivanti dalle interconnessioni fra banche dati centrali e periferiche funzionali alla piena attuazione del federalismo fiscale. Il Garante ha infine osservato come l'art. 71, comma 1-*bis*, del codice dell'amministrazione digitale non preveda il parere del Garante in ordine ai decreti che devono individuare le regole tecniche e di sicurezza per il funzionamento del sistema pubblico di connettività né in ordine agli accordi di servizio e di cooperazione funzionali alla digitalizzazione delle amministrazioni, il che non consente spesso una puntuale verifica delle misure di sicurezza e delle garanzie per la protezione dei dati personali così trattati;

c) il 30 gennaio 2009, presso il Comitato parlamentare per la sicurezza della Repubblica, un'audizione sulla vicenda della raccolta di dati effettuata nell'ambito di una inchiesta giudiziaria della procura di Catanzaro (*cd. "caso Genchi"*).

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

Nel 2009, l'Autorità ha fornito la consueta collaborazione al Governo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

In particolare, sono stati forniti elementi di valutazione ai fini della risposta, da parte del Governo, all'interrogazione n. 4-00050 dell'on. Mecacci ed altri, concernente il *"Foreign Intelligence Surveillance Act"*. In particolare, l'Autorità, dopo avere illustrato la legislazione federale attualmente vigente negli Stati Uniti in materia di intercettazione di comunicazioni, anche nell'ambito di operazioni di *intelligence* finalizzate al contrasto del terrorismo, e i più importanti orientamenti della Corte Suprema in materia, ha evidenziato le possibili implicazioni di tali norme sul diritto alla protezione dei dati personali dei cittadini europei, anche per quanto concerne gli istituti attraverso i quali gli interessati possono far valere i propri diritti.

L'Autorità ha inoltre assicurato la richiesta collaborazione ai fini dell'acquisizione, da parte del Governo, degli elementi utili alla predisposizione di un'informativa urgente, svolta nella seduta n. 179 del 19 maggio 2009 dell'Assemblea della Camera dei deputati, relativa al fenomeno dello *"spionaggio telematico"* attraverso la messaggistica dei telefoni cellulari (*cd.* "*Sms*-spia")-tema oggetto peraltro di diversi atti di sindacato ispettivo.

Il Garante ha in particolare fornito al Governo un rapporto tecnico, basato anche sulle risposte ricevute dai principali produttori di *software* di sicurezza ad un questionario relativo alla vulnerabilità dei telefoni cellulari, illustrando i rischi per il diritto alla protezione dei dati personali connessi a tale fenomeno di controllo a distanza dei telefoni cellulari.

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 5, del Codice), il Garante ha espresso nel periodo in esame diversi pareri i quali hanno riguardato, in particolare:

a) uno schema di regolamento interno del Ministero dell'ambiente e della tutela

del mare per l'utilizzo della posta elettronica e della rete internet negli uffici del ministero (*Parere* 4 marzo 2010 [doc. *web* n. 1706464]);

b) uno schema di decreto del Presidente del Consiglio dei ministri recante regole tecniche per il rilascio - ai dipendenti di ruolo delle amministrazioni pubbliche statali, nonché al personale militare in attività di servizio o in posizione ausiliaria - della tessera personale di riconoscimento di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851, in formato elettronico (*cd.* "modello ATe") (*Parere* 18 febbraio 2010 [doc. *web* n. *1702885*]);

c) uno schema di regolamento di esecuzione del sesto 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]);

d) uno schema di decreto interministeriale 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]);

e) 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. n. 269/2003 (*Parere* 21 gennaio 2010 [doc. *web* n. 1693904]);

f) uno schema di regolamento recante 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]);

g) uno schema di decreto del Ministro della giustizia recante regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, in sostituzione del decreto del Ministro della giustizia del 17 luglio 2008 (*Parere* 16 dicembre 2009 [doc. *web* n. 1689683]);

h) uno schema di documento recante linee-guida per la dematerializzazione della documentazione clinica in diagnostica per immagini, adottato dal Ministero del

lavoro, della salute e delle politiche sociali (*Parere* 26 novembre 2009 [doc. *web* n. 1688961]);

i) uno schema di decreto del Ministro dell'interno concernente le modalità di pubblicazione dei provvedimenti emessi in caso di insussistenza dei presupposti per la proposta di scioglimento dei consigli comunali e provinciali (*Parere* 29 ottobre 2009 [doc. *web* n. 1669219]);

j) uno schema di decreto concernente l'anagrafe dei fondi sanitari istituita, presso il Ministero del lavoro, della salute e delle politiche sociali, dall'art. 9, comma 9, del d.lgs. 30 dicembre 1992, n. 502, e dal successivo decreto ministeriale 31 maggio 2008 (*Parere* 17 settembre 2009 [doc. *web* n. 1655693]);

k) uno schema di circolare predisposta dal Ministro per la pubblica amministrazione e l'innovazione recante *"prime indicazioni operative"* relative alle misure di trasparenza e pubblicità previste dall'art. 21, comma 1, della l. 18 giugno 2009, n. 69 (*Parere* 16 luglio 2009 [doc. *web* n. 1639950]);

l) uno schema di decreto del Presidente della Repubblica recante il *"Testo unico delle disposizioni regolamentari in materia di ordinamento militare"*, elaborato al fine di codificare in un unico testo normativo le fonti di rango secondario di interesse dell'Amministrazione della difesa (art. 14, l. 28 novembre 2005, n. 246) (*Parere* 12 giugno 2009 [doc. *web* n. 1630403]);

m) uno schema di decreto del Ministro degli affari esteri recante aggiornamenti grafici e tecnici del libretto di passaporto, che sostituisce integralmente, abrogandolo, il decreto del Ministro degli affari esteri del 29 novembre 2005 (*Parere* 18 giugno 2009 [doc. *web* n. 1630387]);

n) uno schema di decreto del Ministero degli affari esteri recante disposizioni sul passaporto elettronico, che sostituisce integralmente, abrogandolo, il decreto del Ministro degli affari esteri del 31 marzo 2006 (*Parere* 18 giugno 2009 [doc. *web* n. 1630422]);

o) uno schema di regolamento *ex* art. 17, comma 2, della l. n. 400/1988, predisposto dal Dipartimento per la semplificazione normativa della Presidenza del Consiglio

dei ministri, concernente la semplificazione e il riordino della disciplina dello sportello unico per le attività produttive, emanato in attuazione dell'art. 38, comma 3, del d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla l. 6 agosto 2008, n. 133 (*Parere* 18 giugno 2009 [doc. *web* n. 1630376]);

p) uno schema di ordinanza del Presidente del Consiglio dei ministri, recante disposizioni urgenti dirette a fronteggiare gli eventi sismici verificatisi nella Regione Abruzzo il giorno 6 aprile 2009 (*Parere* 4 giugno 2009 [doc. *web* n. 1621162]);

q) uno schema di decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità e i contenuti delle prove di ammissione a corsi di laurea ad accesso programmato per l'anno accademico 2009/2010 (*Parere* 14 maggio 2009 [doc. *web* n. 1617715]);

r) uno schema di decreto del Ministro del lavoro, della salute e delle politiche sociali recante istituzione del Sistema informativo per la salute mentale (Sism) (*Parere* 6 maggio 2009 [doc. *web* n. 1616893]);

s) uno schema di decreto del Ministro del lavoro della salute e delle politiche sociali recante istituzione del Sistema informativo per le dipendenze (Sind) (*Parere* 6 maggio 2009 [doc. *web* n. 1615306]);

t) uno schema di decreto del Ministro dell'interno in materia di verifica di requisiti ostativi al rilascio di titoli di accesso a competizioni calcistiche (*Parere* 16 aprile 2009 [doc. *web* n. 1615614]);

u) uno schema di decreto del Ministro dell'economia e delle finanze di concerto con il Ministro del lavoro, della salute e delle politiche sociali concernente il controllo delle esenzioni sanitarie per reddito (*Parere* 8 aprile 2009 [doc. *web* n. 1611955]);

v) uno schema di decreto del Ministro dell'istruzione e dell'università e della ricerca riguardante le pre-iscrizioni universitarie per l'anno accademico 2009/2010 (*Parere* 26 marzo 2009 [doc. *web* n. 1606014]);

w) uno schema di decreto del Ministro dell'economia e delle finanze recante il regolamento che disciplina le modalità di accesso al Sistema informativo delle operazioni degli enti pubblici (Siope) (*Parere* 26 febbraio 2009 [doc. *web* n. 1605504]);

x) uno schema di d.P.C.m. recante il regolamento in materia di accesso degli organismi di informazione e sicurezza agli archivi informatici delle pubbliche amministrazioni e di altri soggetti, adottato in attuazione dell'art. 13 della l. 3 agosto 2007, n. 124 (*Parere* 12 febbraio 2009 [doc. *web* n.1597595]).

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità, fra i quali in particolare:

a) il decreto del Ministro del lavoro, della salute e delle politiche sociali 11 dicembre 2009 (in *G.U.* 12 gennaio 2010, n. 8) recante istituzione del Sistema informativo per il monitoraggio degli errori in sanità;

b) l'accordo della Conferenza unificata del 26 novembre 2009 (in *G.U.* 4 gennaio 2010, n. 2), sancito ai sensi dell'art. 9 del d.lgs. 28 agosto 1997, n. 281, sul documento proposto dal Tavolo di consultazione permanente sulla sanità penitenziaria in materia di dati sanitari, flussi informativi e cartella clinica anche informatizzata;

c) il decreto del Ministro dello sviluppo economico del 12 novembre 2009 (in *G.U.* 6 febbraio 2010, n. 30), recante disposizioni relative al servizio del numero telefonico unico di emergenza europeo;

d) il d.P.R. 22 giugno 2009, n. 122 (in *G.U.* 19 agosto 2009, n. 191), recante regolamento per il coordinamento delle norme vigenti per la valutazione degli alunni e ulteriori modalità applicative in materia, ai sensi degli artt. 2 e 3 del d.l. 1° settembre 2008, n. 137, convertito, con modificazioni, dalla l. 30 ottobre 2008, n. 169;

e) il decreto del Ministro del lavoro, della salute e delle politiche sociali, di concerto con il Ministro dell'economia e delle finanze, 19 maggio 2009 n. 46441 (in *G.U.* 22 luglio 2009, n. 168) in materia di accesso all'indennità di disoccupazione per sospensione dell'attività lavorativa;

f) il decreto del Ministro del lavoro, della salute e delle politiche sociali 29 gennaio 2009 (in *G.U.* 4 maggio 2009, n. 101) recante istituzione degli *"Access Point"* per l'applicazione del regolamento (CE) n. 883/2004 del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativo al coordinamento dei sistemi di sicurezza sociale;

g) il decreto del Ministro del lavoro, della salute e delle politiche sociali 18 dicembre 2008 (in *G.U.* 9 marzo 2009, n. 56) recante l'aggiornamento dei sistemi di classificazione adottati per la codifica delle informazioni cliniche contenute nella scheda di dimissione ospedaliera e per la remunerazione delle prestazioni ospedaliere;

h) il decreto del Ministro del lavoro, della salute e delle politiche sociali 17 dicembre 2008 (in *G.U.* 9 gennaio 2009, n. 6), recante istituzione della banca dati finalizzata alla rilevazione delle prestazioni residenziali e semiresidenziali;

i) il decreto del Ministro del lavoro, della salute e delle politiche sociali 17 dicembre 2008 (in *G.U.* 13 gennaio 2009, n. 9) recante istituzione del sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza sanitaria in emergenza-urgenza;

l) il decreto del Ministro del lavoro, della salute e delle politiche sociali 17 dicembre 2008 (in *G.U.* 9 gennaio 2009, n. 6) recante istituzione del sistema informativo per il monitoraggio dell'assistenza domiciliare.

Inoltre, il parere del Garante non è stato richiesto in relazione a provvedimenti i quali, ancorché non prevedano specifiche disposizioni in materia di protezione dei dati personali, tuttavia incidono, sia pur indirettamente, su tale materia. Tra questi provvedimenti si richiamano, in particolare, i seguenti:

a) l'accordo della Conferenza unificata del 26 novembre 2009, sancito ai sensi dell'art. 9 del d.lgs. 28 agosto 1997, n. 281, sul documento proposto dal Tavolo di consultazione permanente sulla sanità penitenziaria in materia di strutture sanitarie nell'ambito del sistema penitenziario italiano (in *G.U.* 4 gennaio 2010, n. 2);

b) l'accordo della Conferenza unificata del 26 novembre 2009, sancito ai sensi dell'art. 9 del d.lgs. 28 agosto 1997, n. 281, sul documento proposto dal Tavolo di consultazione permanente sulla sanità penitenziaria recante linee di indirizzo per l'assistenza ai minori sottoposti a provvedimento dell'autorità giudiziaria (in *G.U.* 4 gennaio 2010, n. 2);

c) il decreto del Ministro del lavoro, della salute e delle politiche sociali del 18 novembre 2009 (*G.U.* 31 dicembre 2009, n. 303), recante istituzione di una rete

nazionale di banche per la conservazione di sangue da cordone ombelicale;

d) il decreto del Ministro del lavoro, della salute e delle politiche sociali del 18 novembre 2009 (in *G.U.* 31 dicembre 2009, n. 303), in materia di conservazione di cellule staminali da sangue del cordone ombelicale per uso autologo-dedicato.

1.2.4. Altri pareri

Su espressa richiesta, il Garante ha espresso parere anche su alcuni altri atti normativi del Governo e, in particolare, sui seguenti provvedimenti:

a) uno schema di disegno di legge predisposto dal Ministero del lavoro, della salute e delle politiche sociali recante l'istituzione dei registri nazionali e dei registri regionali degli impianti protesici mammari, obblighi informativi alle pazienti nonché divieto di plastica mammaria ai minori (*Parere* 16 dicembre 2009 [doc. *web* n. 1689676]);

b) un progetto di Accordo Italia-Usa predisposto dal Ministero degli affari esteri per il rafforzamento della collaborazione bilaterale nella prevenzione e lotta alle forme gravi di criminalità (*"serious crimes"*) (*Parere* 28 maggio 2009 [doc. *web* n. 1624697]).

1.3. LEGGI REGIONALI

Nel corso del 2009 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 (trentaquattro) è stato riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale rispetto ai profili di protezione dei dati personali.

Solo in due casi l'Autorità ha fornito alla Presidenza del Consiglio dei ministri osservazioni in merito alla compatibilità della legge in esame con i princìpi in materia di protezione dei dati personali, ai fini della valutazione sull'eventuale sussistenza

dei presupposti per l'impugnazione della legge regionale.

In particolare, in relazione alla legge della Regione Friuli-Venezia Giulia n. 9 del 29 aprile 2009 (*Disposizioni in materia di politiche di sicurezza e ordinamento della polizia locale*), si è rilevato come l'omessa menzione, in talune disposizioni, del necessario rispetto della legislazione statale in materia di protezione dei dati personali - quale norma interposta ai fini del sindacato di costituzionalità in riferimento all'art. 117, comma secondo, lettera *l*), della Costituzione - rischiasse di violare tale norma costituzionale, giusta il principio sancito dalla Consulta con la sentenza n. 271 del 2005.

In relazione alla legge della Regione Calabria n. 25 del 17 agosto 2009, recante *"Norme per lo svolgimento di elezioni primarie per la selezione di candidati all'elezione del presidente della Giunta regionale"*, si sono rilevate talune perplessità sulla compatibilità della disciplina ivi prevista con la legislazione statale in materia di protezione dei dati personali, da valutare anche ai fini di una possibile violazione del predetto art. 117, comma 2, lett. *l*), della Costituzione. Le criticità evidenziate riguardavano, in particolare, le norme della legge regionale volte a disciplinare taluni adempimenti procedurali funzionali allo svolgimento delle consultazioni elettorali, tali da consentire di desumere la scelta dell'elettore in base alla scheda della lista richiesta.

Le perplessità sollevate dal Garante sono state condivise dal Consiglio dei ministri che ha deliberato di impugnare la suddetta legge regionale, che tuttavia, a distanza di un breve lasso di tempo, è stata modificata, recependo sostanzialmente i rilievi del Governo (leggi della Regione Calabria nn. 38 e 44 del 2009).

2. QUADRO NORMATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

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

L'applicazione - anche in sede giurisdizionale e amministrativa - del Codice ne ha dimostrato l'assoluta rilevanza ai fini della garanzia dei diritti fondamentali e, in particolare, del *"diritto alla protezione dei dati personali"* introdotto nel nostro ordinamento dall'art. 1 del Codice.

Pur nel sostanziale rispetto del suo impianto generale, il Codice ha subito, in particolare nel corso del 2009 e in questo primo scorcio 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 di pubblici funzionari

Una prima significativa modifica al Codice si registra in materia di conoscibilità di notizie relative all'attività del personale che svolge una funzione pubblica, introdotta dall'art. 14 del disegno di legge sul lavoro pubblico (AS 1167-B) approvato dalle Camere il 3 marzo 2010 e rinviato alle stesse dal Presidente della Repubblica.

Il disegno di legge ha integrato l'art. 19 del Codice ed ha contestualmente soppresso la novella introdotta all'art. 1 del medesimo Codice nell'ambito di un ampio intervento normativo in materia di trasparenza dell'attività delle pubbliche amministrazioni, già descritta nella *Relazione 2008*, p. 37 (art. 4, comma 9, l. 4 marzo 2009, n.15, recante delega al Governo per l'ottimizzazione della produttività del lavoro pubblico). Un emendamento d'iniziativa parlamentare aveva infatti modificato il predetto art. 1 (rubricato *"Diritto alla protezione dei dati personali"*) sancendo che *"le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale"*.

Al riguardo, si rammenta che, in seguito all'approvazione di tale norma, il Garante aveva segnalato informalmente al Governo l'opportunità di assicurare, quanto meno, la corretta collocazione sistematica della norma, non già fra i princìpi generali,

bensì nel capo del Codice riguardante i trattamenti effettuati dai soggetti pubblici (art. 19 del Codice), anche in considerazione dei possibili dubbi di legittimità costituzionale e comunitaria della disposizione, che sottraeva sostanzialmente talune categorie di informazioni e i relativi soggetti interessati alle garanzie in materia di protezione dei dati personali. Inoltre, al fine di rendere più facilmente applicabile la norma, l'Autorità aveva richiamato l'attenzione del Governo sull'opportunità di demandare a un successivo decreto l'individuazione delle notizie relative alle prestazioni lavorative oggetto della disposizione.

Tali indicazioni sono state recepite dal Governo e trasfuse in un emendamento, poi presentato dal relatore al disegno di legge in esame, volto a sopprimere la modifica apportata all'art. 1 del Codice, e a demandare a un regolamento, emanato previa acquisizione del parere del Garante, l'individuazione delle notizie concernenti lo svolgimento delle prestazioni dei pubblici funzionari di cui è ammessa la comunicazione.

Nel corso dei lavori, la proposta emendativa ha, tuttavia, subito dei correttivi, fino alla versione definitivamente approvata che prevede l'accessibilità delle notizie riguardanti le prestazioni e la relativa valutazione, salvo che si tratti di alcune informazioni per lo più di natura sensibile. In base al nuovo comma 3-*bis* dell'art. 19 del Codice, infatti, *"le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'Amministrazione di appartenenza. Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'Amministrazione"* idonee a rivelare dati sensibili.

2.1.2. Le modifiche in materia di comunicazione promozionale

Un altro importante intervento modificativo del Codice ha riguardato la disciplina dell'attività di comunicazione promozionale effettuata mediante l'impiego del telefono.

L'art. 20-*bis* del d.l. 25 settembre 2009, n. 135, convertito, con modificazioni, dalla l. 20 novembre 2009, n. 166 (recante disposizioni urgenti per l'attuazione di obblighi comunitari) ed introdotto da un emendamento di iniziativa parlamentare, ha integrato

l'art. 130 del Codice (*"Comunicazione indesiderate"*) prevedendo che il trattamento, mediante l'impiego del telefono, di dati personali provenienti da elenchi telefonici a disposizione del pubblico sia consentito solo nei confronti di chi non abbia esercitato il diritto di opposizione iscrivendo la numerazione telefonica di cui è intestatario in un apposito registro pubblico (*cd. "opt-out"*).

La norma prevede pertanto l'istituzione, con regolamento del Governo, entro sei mesi dall'entrata in vigore della legge di conversione del decreto-legge, di un registro pubblico delle opposizioni - destinato a operare sotto la vigilanza del Garante - iscrivendosi al quale ciascun cittadino potrà esercitare, appunto, il diritto di opposizione a ogni trattamento dei suoi dati effettuato per telefono a fini di comunicazione promozionale (in particolare: *"a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale"* - art. 7, comma 4, lett. *b*), del Codice).

Nell'esercizio della potestà regolamentare, il Governo dovrà attenersi ai seguenti princìpi: il registro può essere istituito e gestito da un ente o un'autorità pubblica titolare di competenze in materia, ovvero affidato - per quanto concerne la realizzazione e la gestione - a un privato mediante contratto di servizio; deve consentire di effettuare esclusivamente interrogazioni selettive (ma non di trasferire i dati ivi contenuti) e tracciare gli accessi; devono essere individuate la tempistica e le modalità d'iscrizione al registro, garantendone l'efficacia indefinita e la revocabilità gratuita e in ogni tempo, prevedendo altresì l'obbligo, in capo a coloro che contattano telefonicamente un utente a fini di comunicazione promozionale, di consentire, da un lato, l'identificazione della linea chiamante e, dall'altro, di informare l'abbonato della possibilità, per il futuro, di opporsi alle chiamate indesiderate mediante l'iscrizione nel registro. Infine, nonostante l'iscrizione al registro, è consentito il trattamento di dati lecitamente raccolti ai sensi degli artt. 23 e 24 del Codice.

La violazione del diritto di opposizione esercitato nelle forme descritte e in quelle che saranno previste dal regolamento di attuazione è punita ai sensi del comma 2-*bis* dell'art. 162 del Codice (comma aggiunto dall'art. 44 del d.l. 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla l. 27 febbraio 2009, n. 14), come novellato dal

medesimo art. 20-*bis*, del d.l. n. 135/2009 (il minimo edittale della sanzione applicabile è ridotto da 20.000 a 10.000 euro) (*cfr. par.* 2.1.3.).

Il dato più significativo della novella consiste dunque nell'avere sostituito 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"*), rendendo necessario l'esercizio del diritto di opposizione (*cd. "opt-out"*).

In proposito il Garante, con un comunicato stampa, ha sottolineato gli effetti negativi dell'emendamento approvato dal Senato sulle telefonate promozionali, che finirà col danneggiare lo stesso *marketing* telefonico facendolo apparire sempre più invadente e insopportabile.

Il Garante ha espresso perplessità anche sulla scelta delle modalità di esercizio del diritto di opposizione, in quanto registri del tipo di quello previsto dal legislatore italiano non hanno in realtà funzionato in nessun paese dove sono stati istituiti, mentre sono facilmente prefigurabili le oggettive difficoltà che molti cittadini, soprattutto anziani, troveranno nel manifestare il loro *"dissenso"* alla comunicazione commerciale.

Infine, l'art. 20-*bis* ha prorogato sino al medesimo termine di sei mesi, la possibilità, per coloro che prima del 1° agosto 2005 avevano costituito banche dati sulla base di elenchi telefonici pubblici, di utilizzare i dati personali contenuti nei medesimi elenchi per fini promozionali anche in deroga alle disposizioni del Codice relative all'informativa e al consenso degli interessati (artt. 13 e 23), secondo la disciplina *"transitoria"* (efficace cioè fino al 31 dicembre 2009) introdotta dal comma 1-*bis* del *cit.* art. 44 del d.l. n. 207/2008, e in relazione alla quale il Garante ha impartito specifiche prescrizioni ai titolari delle banche dati con *provvedimento* 12 marzo 2009.

Sul punto, è opportuno ricordare che il 7 aprile 2009 la Commissione europea, rispondendo ad un'interrogazione parlamentare (P-1463/2009, on. Cappato), ha rilevato il contrasto tra la norma di cui al suddetto art. 44, comma 1-*bis*, del d.l. n. 207/2008 e le prescrizioni adottate in merito dal Garante quale autorità nazionale deputata alla garanzia del diritto alla protezione dei dati personali, preannunciando una consultazione con le autorità italiane al fine di verificarne la compatibilità con il diritto comunitario

e in particolare con la Direttiva n. 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche.

Invero, con nota C (2010)290 del 28 gennaio 2010, la Commissione europea, nell'ambito della procedura di infrazione 2009/2356, ha disposto una costituzione in mora, *ex* art. 258 del Trattato sul funzionamento dell'Unione europea, nei confronti del nostro Paese, ritenendo che le novelle apportate alla disciplina sul *telemarketing* dai d.l. nn. 207/2008 e 135/2009, non garantiscano, per alcuni aspetti, il corretto recepimento delle pertinenti norme della direttiva 2002/58/CE.

2.1.3. Le modifiche in materia di sanzioni

Si segnalano, infine, mirati interventi modificativi del quadro sanzionatorio previsto dal Codice, cui si è già fatto cenno, seppure indirettamente, nel paragrafo precedente.

Il già citato art. 20-*bis* del d.l. 25 settembre 2009, n. 135, convertito, con modificazioni, dalla l. 20 novembre 2009, n. 166, ha infatti previsto la punibilità con sanzione amministrativa della violazione del diritto di opposizione esercitato nelle nuove forme previste dall'art. 130, comma 3-*bis*, del Codice e dal relativo regolamento di attuazione (cioè mediante iscrizione nell'apposito registro pubblico delle opposizioni) (art. 162, comma 2-*quater*, del Codice). In tali casi si applica la sanzione pecuniaria prevista dal comma 2-*bis* del medesimo art. 162 del Codice (*"Altre fattispecie"*) che lo stesso decreto-legge ha ridotto nel minimo edittale da 20.000 a 10.000 euro.

Tale ultimo intervento sull'entità della sanzione, che riguarda anche le altre fattispecie previste nel medesimo comma 2-*bis* dell'art. 162 (trattamento di dati personali effettuato in violazione dell'obbligo di adottare le misure minime di sicurezza ai sensi dell'art. 33 del Codice, essendo peraltro in tal caso escluso il pagamento in misura ridotta; violazione delle disposizioni richiamate nell'art. 167 del Codice concernente il trattamento illecito di dati personali), mira a calibrare meglio la portata della sanzione rispetto a fatti di lieve entità, segnatamente nel caso in cui le violazioni siano commesse da piccole realtà produttive.

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

Nel corso del 2009 sono stati approvati alcuni provvedimenti normativi che hanno riguardato il trattamento dei dati personali e l'attività del Garante.

Vanno ricordati, in particolare:

- il disegno di legge recante *"Deleghe al Governo in materia di lavori usuranti, di riorganizzazione di enti, di congedi, aspettative e permessi, di ammortizzatori sociali, di servizi per l'impiego, di incentivi all'occupazione, di apprendistato, di occupazione femminile, nonché misure contro il lavoro sommerso e disposizioni in tema di lavoro pubblico e di controversie di lavoro"*, approvato dalle Camere il 3 marzo 2010 e rinviato alle stesse dal Presidente della Repubblica, oltre ad apportare rilevanti modifiche agli artt. 1 e 19 del Codice, ha introdotto diverse disposizioni d'interesse sotto il profilo della protezione dei dati personali, e in particolare:

  a) l'art. 5 del disegno di legge integra l'art. 21 della l. 18 giugno 2009, n. 69, che, come è noto, ha sancito, in capo alle pubbliche amministrazioni, 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 fu a suo tempo sentita dal Ministro per la pubblica amministrazione e l'innovazione in ordine alla compatibilità di simili disposizioni con il diritto alla protezione dei dati personali e, più recentemente, ha espresso parere sullo schema di circolare adottata dal predetto Ministro per l'attuazione della norma (*cfr. par.* 1.2.3.). In base alla nuova disposizione (art. 21, comma 1-*bis*, l. n. 69/2009) le pubbliche amministrazioni devono comunicare i predetti dati alla Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica, per via telematica e secondo i criteri e le modalità che saranno individuati con circolare del Ministro per la pubblica amministrazione e l'innovazione, che li pubblica nel proprio sito istituzionale;

Trasparenza dei dati relativi ai dirigenti pubblici

Permessi di lavoro per assistenza a portatori di *handicap*

b) l'art. 24 del disegno di 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 in base alla legge, che dovranno essere 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 della legittima fruizione dei permessi *"di rilevante interesse pubblico"* e individua le operazioni di trattamento che possono essere effettuate dalle amministrazioni a tali fini, nonché termini di conservazione dei dati stessi (due anni nella banca dati; trenta 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 del disegno di legge, nel quadro delle misure di controllo sulle assenze dal luogo di lavoro, disciplina l'invio per via telematica dei certificati di malattia di 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 del disegno di 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 in 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, d.lgs. n. 165/2001, art. 15 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; 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;

Digitalizzazione della giustizia: 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 in particolare, demanda a uno o più regolamenti 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. Lo stesso articolo estende l'uso della posta elettronica certificata a tutte le comunicazioni e le notificazioni per via telematica nei processi civili e penali. La trasmissione telematica degli atti

(all'indirizzo di posta elettronica certificata) riguarderà, nel processo civile, le notificazioni e le comunicazioni alle parti costituite in giudizio e ai consulenti tecnici nonché le notificazioni e comunicazioni previste dalla legge fallimentare e, nel processo penale, le notificazioni a persona diversa dall'imputato disciplinate da specifiche disposizioni del codice di rito. Si prevede che la notificazione o comunicazione che contiene dati sensibili è effettuata solo per estratto con contestuale messa a disposizione, sul sito internet individuato dall'amministrazione, dell'atto integrale cui il destinatario può accedere con strumenti elettronici. Per quanto riguarda la fase esecutiva del processo civile, sia relativamente all'espropriazione mobiliare sia a quella immobiliare, si autorizza il giudice ad effettuare con modalità telematiche il versamento della cauzione, la presentazione delle offerte, lo svolgimento della gara e l'incanto nonché il pagamento del prezzo. Al fine di consentire la piena attuazione del processo telematico, si prevede che nell'albo degli avvocati sia indicato, oltre al codice fiscale, l'indirizzo di posta elettronica certificata del difensore. Gli indirizzi di posta elettronica certificata e i codici fiscali, aggiornati con cadenza giornaliera, sono resi disponibili per via telematica al Consiglio nazionale forense e al Ministero della giustizia nelle forme previste dalle predette regole tecniche. Il *cit.* art. 4 autorizza inoltre il Ministro della giustizia ad adottare un regolamento al fine di disciplinare la tipologia e le modalità di estrazione, raccolta e trasmissione dei dati statistici dell'Amministrazione della giustizia all'archivio informatico centralizzato esistente. Si segnala peraltro che, prima dell'entrata in vigore del decreto-legge in esame, il Garante ha reso *parere* [doc. *web* n. 1689683] (*cfr. par.* 1.2.3.) su di uno schema di decreto recante *"Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, in sostituzione del decreto del Ministro della giustizia del 17 luglio 2008"*, che è stato necessario modificare in ragione di precedenti variazioni del quadro normativo (artt. 16 e 16-*bis*, d.l. 29 novembre 2008 n. 185, convertito, con modificazioni, dalla l. 28 gennaio 2009, n. 2; art. 137 c.p.c., come novellato dall'art. 45, comma 18, l. 18 giugno 2009, n. 69), nonché delle indicazioni espresse dal Cnipa in occasione dell'approvazione dei precedenti schemi di decreti;

Accertamento e riscossione di tributi locali: dati anagrafici

- il d.l. 30 dicembre 2009, n. 195, convertito, con modificazioni, dalla l. 26 febbraio 2010, n. 26, recante disposizioni urgenti per la cessazione dello stato di emergenza in materia di rifiuti nella Regione Campania e per l'avvio della fase *post*-emergenziale nel territorio della Regione Abruzzo, il cui art. 11, comma 3, ha posto in capo ai comuni della Regione Campania l'obbligo di trasmettere alle province (per l'eventuale successivo inoltro alle società provinciali di cui alla legge della Regione Campania 28 marzo 2007, n. 4, preposte all'accertamento e alla riscossione) i dati necessari ai fini della riscossione della tassa per lo smaltimento dei rifiuti solidi urbani (Tarsu) e della tariffa integrata ambientale (Tia), tra i quali la banca dati aggiornata al 31 dicembre 2008 dell'anagrafe della popolazione riportante, in particolare, le informazioni sulla residenza e sulla composizione del nucleo familiare degli iscritti. I medesimi comuni dovranno periodicamente comunicare gli aggiornamenti dei dati contenuti in tale banca dati;

Carta d'identità: consenso o diniego alla donazione degli 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 della persona cui si riferisce a donare i propri organi in caso di morte;

Tessera di riconoscimento dei militari

- il d.l. 4 novembre 2009, n. 152, in materia di missioni internazionali delle Forze armate e di polizia, convertito dalla l. 29 dicembre 2009, n. 197, e successive modificazioni, il cui art. 3, comma 2, dispone che al fine di agevolare le prime operazioni di soccorso medico, relativamente all'impiego in missioni internazionali o in altre situazioni di potenziale esposizione a pericolo, la tessera di riconoscimento del personale militare, rilasciata in formato elettronico ai sensi dell'art. 66, comma 8, del codice dell'amministrazione digitale, previo consenso dell'interessato al trattamento dei dati personali, contiene i dati *"sanitari di emergenza, quali lo stato vaccinale, le terapie in atto, le allergie, le intolleranze, gli impianti, le trasfusioni"*. La medesima tessera di riconoscimento può contenere anche il consenso del militare

alla donazione degli organi. Con decreto del Ministro della difesa, sentito il Garante, saranno individuate le modalità di caricamento dei dati nella tessera, i livelli e le modalità di accesso selettivo ai dati, nonché le specifiche misure volte a garantire la sicurezza dei dati ivi inclusi. L'Autorità ha collaborato alla stesura delle norma in esame per i profili inerenti alla protezione e alla sicurezza dei dati;

- il d.l. 25 settembre 2009, n. 134, convertito, con modificazioni, dalla l. 24 novembre 2009, n. 167, recante *"Disposizioni urgenti per garantire la continuità del servizio scolastico ed educativo per l'anno 2009-2010"*, che contiene alcune importanti disposizioni in materia di anagrafe degli studenti, trattamenti di sostegno al reddito e Borsa continua nazionale del lavoro.

In particolare:

Anagrafe degli studenti

a) l'art. 1-*quater* del decreto-legge, nel novellare l'art. 3, comma 1, del d.lgs. 15 aprile 2005, n. 76, ha ricompreso, tra le informazioni trattate dall'Anagrafe nazionale degli studenti presso il Ministero dell'istruzione, dell'università e della ricerca, anche i dati relativi alla valutazione degli studenti, autorizzando altresì il medesimo Ministero ad acquisire dalle istituzioni scolastiche statali e paritarie *"i dati personali, sensibili e giudiziari degli studenti e altri dati utili alla prevenzione e al contrasto della dispersione scolastica"*. L'Autorità ha collaborato alla stesura del decreto ministeriale in vista della espressione del proprio parere sul relativo schema;

Trattamenti di sostegno al reddito

b) l'art. 1, comma 4-*terdecies*, nel novellare l'art. 19, comma 4, del d.l. 29 novembre 2008, n. 185, convertito, con modificazioni, dalla l. 28 gennaio 2009, n. 2, ha sancito che nella banca dati costituita presso l'Inps ed ivi prevista, *"confluiscono tutti i dati disponibili relativi ai percettori di trattamenti di sostegno al reddito e ogni altra informazione utile per la gestione dei relativi trattamenti"*, disponendo altresì che a tale archivio possono accedere, tra gli altri, anche le regioni, il Ministero del lavoro, della salute e delle politiche sociali, la società Italia lavoro S.p.A. e l'Istituto per lo sviluppo della formazione professionale dei lavoratori;

Domanda e offerta di lavoro

c) l'art. 1, comma 4-*quaterdecies*, ai fini di cui al suddetto comma 4-*terdecies*, nel novellare il d.lgs. 10 settembre 2003, n. 276, ha attribuito ai servizi della Borsa continua nazionale del lavoro la funzione di provvedere, a livello nazionale, (oltre che alla definizione, anche) alla raccolta, alla comunicazione e alla diffusione dei dati che permettono la massima efficienza e trasparenza del processo di incontro tra domanda e offerta di lavoro, assicurando anche gli strumenti tecnologici necessari per la raccolta e la diffusione delle informazioni presenti nei siti internet. Conseguentemente, la citata disposizione ha abrogato i commi 1 e 2 dell'art. 8 del suddetto d.lgs. n. 276/2003, che imponevano alle agenzie per il lavoro e agli altri operatori pubblici e privati autorizzati o accreditati di assicurare ai lavoratori il diritto di indicare i soggetti o le categorie di soggetti ai quali i propri dati personali devono essere comunicati, anche ai fini *"del pieno soddisfacimento del diritto al lavoro"* e, rispettivamente, prescrivevano il parere del Garante in ordine al decreto che il Ministro del lavoro e delle politiche sociale avrebbe dovuto emanare entro sessanta giorni dalla data di entrata in vigore dello stesso decreto legislativo, al fine di disciplinare le modalità di trattamento dei dati personali previsti dal medesimo decreto;

- il d.l. 1° luglio 2009, n. 78, recante *"Provvedimenti anticrisi, nonché proroga di termini e della partecipazione italiana a missioni internazionali"*, convertito, con modificazioni, dalla l. 3 agosto 2009, n. 102. Nel corso dell'esame, in prima lettura, del disegno di legge di conversione sono stati presentati in Commissione alcuni emendamenti d'iniziativa parlamentare volti a introdurre significative modifiche al Codice in materia di: nozione di dato sensibile; applicabilità delle norme del Codice alle persone giuridiche; semplificazione degli adempimenti relativi alle misure minime di sicurezza, in particolare per quanto riguarda il documento programmatico sulla sicurezza. Al riguardo, l'Ufficio del Garante ha segnalato al Dipartimento per la funzione pubblica della Presidenza del Consiglio dei ministri le forti perplessità dell'Autorità su tali proposte emendative, per le implicazioni sulla protezione dei dati personali dei cittadini, anche alla luce del quadro normativo europeo.

Gli emendamenti sono stati comunque dichiarati inammissibili per estraneità di materia. Il decreto-legge prevede talune norme d'interesse, con particolare riferimento all'istituzione di nuove banche dati.

In particolare:

Banca dati per studi economico-sociali

a) l'art. 11, *"Analisi e studi economico-sociali"*, sancisce la possibilità di utilizzo *"in modo coordinato ed integrato"* dei sistemi informativi del Ministero dell'economia e delle finanze, del Ministero del lavoro, della salute e delle politiche sociali nonché dei soggetti ad essi collegati o da essi vigilati o controllati, al fine di realizzare - *"nel rispetto dei princìpi vigenti in materia di trattamento dei dati nell'ambito del sistema statistico nazionale"* e *"della normativa sulla protezione dei dati personali"* - una banca dati unitaria funzionale ad analisi e studi mirati alla elaborazione delle politiche economiche e sociali. Il richiamo al rispetto delle norme del Codice induce a ritenere che tale archivio informatico contenga anche dati personali;

Potenziamento della riscossione

b) l'art. 15, *"Potenziamento della riscossione"*, introduce strumenti idonei a potenziare ulteriormente l'efficacia delle attività di riscossione da parte dell'amministrazione finanziaria. In particolare, il comma 1 impone all'amministrazione finanziaria ed a ogni altra amministrazione pubblica, di inviare all'Inps e agli altri enti di previdenza e assistenza obbligatoria, in via telematica e in forma disaggregata per singola tipologia di redditi, le informazioni in loro possesso utili a determinare l'importo delle prestazioni previdenziali ed assistenziali collegate al reddito dei beneficiari, relative a titolari, e rispettivi coniugi e familiari, di prestazioni pensionistiche o assistenziali residenti in Italia. Si precisa espressamente che la comunicazione deve avvenire nel rispetto della *"normativa in materia di dati personali"*. Il comma 8-*quinquies*, nel modificare l'art. 32 del decreto del Presidente della Repubblica 29 settembre 1973, n. 600, e successive modificazioni, autorizza gli uffici delle imposte a richiedere ad autorità ed enti - con modalità stabilite con un decreto di natura non regolamentare di successiva emanazione - notizie, dati, documenti e informazioni di natura creditizia, finanzia-

ria e assicurativa, relativi alle attività di controllo e di vigilanza dagli stessi svolte, *"anche in deroga a specifiche disposizioni di legge"*. Il comma 8-*sexies*, nel modificare l'art. 51 del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, autorizza parimenti gli uffici dell'imposta sul valore aggiunto a richiedere ad autorità ed enti - con modalità stabilite con un decreto di natura non regolamentare di successiva emanazione - notizie, dati, documenti e informazioni di natura creditizia, finanziaria e assicurativa, relativi alle attività di controllo e di vigilanza svolte dagli stessi organi, *"anche in deroga a specifiche disposizioni di legge"*. Il comma 8-*octies*, nel modificare l'art. 7 della l. 9 luglio 1990, n. 187, impone al Pra di effettuare una specifica segnalazione all'Agenzia delle entrate, al Corpo della Guardia di finanza e alla regione territorialmente competente, relativa al fatto che una singola persona fisica risulti proprietaria di dieci o più veicoli;

Contrasto del gioco illegale

c) l'art. 15-*ter*, *"Piano straordinario di contrasto del gioco illegale"*, istituisce presso l'Amministrazione autonoma dei monopoli di Stato un'apposita banca dati, alimentata da tutte le informazioni derivanti dall'ordinaria gestione dei giochi pubblici, nonché *"dall'attività di controllo da chiunque effettuata e da qualunque altra fonte conoscitiva"*. Tale archivio è finalizzato a consentire, attraverso lo studio e l'elaborazione, anche tecnico-statistica, delle informazioni in esso contenute, la rilevazione di possibili indici di anomalia e di rischio, idonei ad agevolare le attività di gioco illegali;

Contrasto alle frodi in materia di invalidità civile

d) l'art. 20, *"Contrasto alle frodi in materia di invalidità civile"*, attribuendo all'Inps la funzione di accertare la permanenza dei requisiti sanitari nei confronti dei titolari di invalidità civile, cecità civile, sordità civile, *handicap* e disabilità, conferisce al medesimo ente la competenza a ricevere (e a comunicare successivamente alle Asl, per via telematica) le domande volte ad ottenere i benefici collegati alla condizione di invalidità, complete della certificazione medica attestante la natura delle infermità invalidanti. Con apposita convenzione tra le regioni e l'Inps saranno disciplinati *"gli aspetti tecnico-procedurali dei flussi*

informativi necessari per la gestione del procedimento per l'erogazione dei trattamenti connessi allo stato di invalidità civile";

Segnalazioni delle autorità indipendenti

- la l. 23 luglio 2009, n. 99, recante *"Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia"*, che contiene una norma in base alla quale il Governo, nel presentare alle Camere il previsto disegno di legge annuale per il mercato e la concorrenza, deve tenere conto anche delle segnalazioni eventualmente trasmesse dall'Autorità garante della concorrenza e del mercato e valutare altresì i pareri resi e le indicazioni contenute nella relazione annuale di tale autorità, nonché le indicazioni di altre autorità amministrative indipendenti (art. 47, comma 3, lettera *a*);

Sicurezza pubblica

- la l. 15 luglio 2009, n. 94 in materia di sicurezza pubblica, nel cui ambito sono state inserite, anche su iniziativa parlamentare, alcune disposizioni d'interesse:

  a) l'art. 1, comma 20, in base al quale coloro che forniscono un servizio di *"money transfer"* devono conservare per dieci anni copia del titolo di soggiorno del cittadino extracomunitario che effettua l'operazione;

  b) l'art. 2, comma 19, il quale, integrando l'art. 38 del codice dei contratti pubblici, prevede la pubblicazione, sul sito dell'Osservatorio sui contratti pubblici, della comunicazione relativa alla mancata denuncia, da parte di persone fisiche, di fatti di concussione o estorsione aggravate di cui siano stati vittime;

  c) l'art. 2, comma 25, il quale integrando l'art. 41-*bis*, comma 2-*quater*, della l. n. 354 del 1975, sul particolare regime penitenziario previsto nei confronti di detenuti per reati gravi, prevede che i colloqui dei detenuti siano comunque videoregistrati;

  d) l'art. 3, commi 38 e 39, che istituisce presso il Ministero dell'interno il registro nazionale delle persone senza fissa dimora, destinato a funzionare attraverso l'utilizzo del sistema Ina-Saia. L'Autorità ha assicurato la collaborazione nella stesura del decreto ministeriale attuativo di tale disposizione, in vista dell'espressione del parere previsto sul relativo schema;

Legge comunitaria 2008

- la l. 7 luglio 2009, n. 88 (legge comunitaria per il 2008), recante delega per l'attuazione, fra l'altro, di direttive europee in materia di dispositivi medici (art. 8 - Direttiva n. 2007/47/CE), di parità di trattamento fra uomini e donne in materia di occupazione (art. 9 - Direttiva n. 2006/54/CE) e di servizi nel mercato interno (art. 41 - Direttiva n. 2006/123/CE *cd. "direttiva servizi"*), nonché per l'attuazione di decisioni quadro adottate nell'ambito della cooperazione di polizia e giudiziaria in materia penale (art. 49). Fra queste assume particolare importanza la decisione-quadro 2006/960/GAI in materia di scambio di informazioni e *intelligence* fra le autorità degli Stati Ue competenti in materia - anche al fine di favorire l'accertamento di reati tra i quali quelli *"connessi al furto di identità relativo ai dati personali"* - la cui attuazione deve comunque prevedere misure volte a salvaguardare la tutela dei dati personali (art. 51, comma 1, lett. *e*));

Adesione al Trattato di Prüm: banca dati nazionale del DNA

- la l. 30 giugno 2009, n. 85 (Adesione al Trattato di Prüm, istituzione della banca dati nazionale del Dna e disposizioni in materia di accertamenti idonei ad incidere sulla libertà personale), che prevede l'istituzione, presso il Ministero dell'interno, di una banca dati nazionale del Dna, in cui confluiranno i profili del Dna tratti da tracce biologiche acquisite nel corso di procedimenti penali e quelli di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati, nonché di soggetti sottoposti a misure limitative della libertà personale. Il controllo sulla suddetta banca dati è affidato al Garante. La legge ricalca sostanzialmente il disegno di legge d'iniziativa governativa approvato nella scorsa legislatura (AS 1877), su cui il Garante aveva reso *parere* (doc. *web* n. 1448799), oltre che una segnalazione (doc. *web* n. 1456163). Essa recepisce parte delle osservazioni rese dal Garante e volte ad assicurare il rispetto della dignità della persona e il principio della proporzionalità del trattamento; altre garanzie saranno individuate con successivi atti regolamentari che saranno adottati sentito il Garante o d'intesa con l'Autorità. Tra le raccomandazioni del Garante che invece non sono state tenute in adeguata considerazione si segnalano in particolare quelle relative all'ampiezza dei cittadini soggetti a prelievo forzoso, nonché ai termini

eccessivamente lunghi previsti per la conservazione dei dati. L'Autorità ha assicurato la più ampia collaborazione nella stesura del regolamento volto a disciplinare, in particolare, il funzionamento e l'organizzazione della banca dati nazionale del Dna e del laboratorio centrale per la banca dati nazionale del Dna, le modalità di trattamento e di accesso per via informatica e telematica ai dati in essi raccolti, nonché le modalità di comunicazione dei dati e delle informazioni richieste;

Informatizzazione della p.a. e pubblicazione *online* di atti

- la l. 18 giugno 2009, n. 69, in materia di sviluppo economico, semplificazione e processo civile, che ha introdotto numerose norme in materia di informatizzazione della pubblica amministrazione e pubblicazione *online* degli atti giudiziari.

  Si richiamano in particolare le seguenti disposizioni:

  a) l'art. 21 ha sancito, in capo alle pubbliche amministrazioni, 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. L'Autorità è stata a suo tempo sentita dal Ministro per la pubblica amministrazione e l'innovazione in ordine alla compatibilità di simili disposizioni con il diritto alla protezione dei dati personali e, più recentemente, ha espresso parere sullo schema di circolare adottata dal predetto Ministro per l'attuazione della norma;

  b) l'art. 23, che incentiva la diffusione di *"buone prassi"* nelle p.a. anche mediante la loro pubblicazione nei siti telematici istituzionali;

  c) l'art. 32, in base al quale gli obblighi di pubblicazione di atti e di provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei siti informatici delle p.a.;

  d) l'art. 33, che reca delega al Governo per la modifica del codice dell'amministrazione digitale, in particolare per quanto riguarda la firma digitale, l'utilizzo del *web* per le comunicazioni fra le amministrazioni e i propri dipendenti, la pubblicazione nei siti di *"indicatori di prestazioni"*;

  e) l'art. 36, che accelera la diffusione del Sistema pubblico di connettività mediante un piano triennale di competenza del Ministro della pubblica amministrazione

e dell'innovazione, volto ad assicurare *"la piena interoperabilità delle banche dati, dei registri e delle anagrafi"* al fine di migliorare i servizi ai cittadini e aumentare l'efficienza delle p.a.;

f) l'art. 37, che agevola il rilascio della Carta nazionale dei servizi (Cns). A tal proposito si sottolinea come l'Autorità abbia collaborato con la Presidenza del Consiglio dei ministri-Dipartimento per la pubblica amministrazione e l'innovazione, per la messa a punto di un decreto per il rilascio ai dipendenti pubblici di una tessera di riconoscimento (modello ATe.), avente anche le funzionalità della Cns, in vista dell'espressione del previsto parere;

g) l'art. 45, comma 16, recante modifiche al codice di procedura civile in materia di pubblicazione di atti giudiziari anche su siti internet;

Voto domiciliare

- la l. 7 maggio 2009, n. 46, volta a consentire l'esercizio del diritto di voto (nella modalità *"domiciliare"*) agli elettori affetti da infermità che ne rendano impossibile l'allontanamento dall'abitazione, in base alla quale i cittadini interessati, al fine di avvalersi di tale possibilità, devono far pervenire al sindaco del comune nelle cui liste elettorali sono iscritti, tra l'altro, un certificato medico attestante l'esistenza delle condizioni d'infermità richieste quali presupposti del voto domiciliare, con prognosi di almeno sessanta giorni decorrenti dalla data di rilascio del certificato, ovvero delle condizioni di dipendenza continuativa e vitale da apparecchi elettromedicali. Si segnala che il testo originario della proposta di legge (AC 907, Bernardini), imponeva in capo all'elettore l'obbligo di trasmettere all'ufficio elettorale del comune copia del certificato rilasciato dalla commissione medica prevista dalla l. n. 104/1992, dal quale risultasse l'esistenza della minorazione, nonché un certificato del medico di base *"in cui si dichiara la persistenza della situazione di gravità e che l'elettore è impossibilitato ad allontanarsi autonomamente dalla propria dimora, indicandone anche la motivazione"*;

Federalismo fiscale

- la l. 5 maggio 2009, n. 42, recante delega al Governo per l'attuazione del federalismo fiscale, che prevede, tra i princìpi e criteri direttivi cui dovranno uniformarsi i decreti legislativi di attuazione, anche la *"definizione di modalità che*

assicurino a ciascun soggetto titolare del tributo l'accesso diretto alle anagrafi e a ogni altra banca dati utile alle attività di gestione tributaria, assicurando il rispetto della normativa a tutela della riservatezza dei dati personali" (art. 2, comma 2, lett. *v*)). La stessa legge ha inoltre istituito la *"Commissione tecnica paritetica per l'attuazione del federalismo fiscale"*, quale *"sede di condivisione delle basi informative finanziarie, economiche e tributarie"* (art. 4), a dimostrazione della rilevanza dello scambio dei dati tra *database*, ai fini della riarticolazione del sistema tributario in relazione ai diversi livelli di governo;

Trasparenza dell'azione amministrativa

- la l. 4 marzo 2009, n. 15 recante delega al Governo per l'ottimizzazione della produttività del lavoro pubblico, che prevede un ampio intervento in materia di trasparenza dell'attività delle pubbliche amministrazioni. La legge sancisce che la trasparenza costituisce livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a norma dell'art. 117, comma 2, lett. *m*), della Costituzione. A tal fine essa è intesa come accessibilità totale, anche attraverso lo strumento dei siti internet delle p.a., delle informazioni concernenti ogni aspetto dell'organizzazione delle pubbliche amministrazioni, dei risultati delle attività di misurazione e valutazione svolte dagli organi competenti, allo scopo di favorire forme diffuse di controllo del rispetto dei princìpi di buon andamento e imparzialità. Le amministrazioni sono tenute ad adottare ogni iniziativa utile a promuovere la massima trasparenza nella propria organizzazione e nella propria attività (art. 4, commi 6-8); in particolare, in materia di valutazione, quale criterio di delega si prevede la disponibilità mediante internet dei *"dati sui quali si basano le valutazioni"* (art. 4, comma 2, lett. *h*)). In tale quadro un emendamento d'iniziativa parlamentare - come già rilevato nel *par.* 2.1.1. - ha introdotto una modifica al Codice, tesa a sancire la conoscibilità delle notizie inerenti lo svolgimento delle prestazioni lavorative in ambito pubblico e la relativa valutazione. Il d.lgs. n. 150/2009, emanato in attuazione della suddetta delega, ha poi previsto, in particolare: la comunicazione via e-mail dei documenti relativi ai procedimenti disciplinari; la trasmissione telematica, nel rispetto delle norme sancite dal Codice, dei certificati medici relativi ad assenze per malattie;

la comunicazione in via telematica, all'amministrazione di appartenenza, della sentenza penale emessa nei confronti di un lavoratore pubblico; l'obbligo, per il personale a contatto con il pubblico, di esposizione di cartellini o targhe identificativi;

- il d.l. 23 febbraio 2009 n. 11, convertito con modificazioni dalla l. 23 aprile 2009, n. 38, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, alla cui stregua:

Sicurezza urbana e videosorveglianza

a) i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico *"per la tutela della sicurezza urbana"* e possono conservare i dati e le immagini raccolti al massimo per sette giorni, fatte salve speciali esigenze di conservazione (art. 6, commi 7 e 8). In sede di esame in seconda lettura, al Senato, del disegno di legge di conversione del decreto-legge, erano stati presentati taluni emendamenti d'iniziativa parlamentare (respinti sia in Aula che in Commissione), volti a sancire l'applicabilità, ai dati raccolti mediante video-sorveglianza, delle norme sulla conservazione dei dati di traffico previste dal Codice (in particolare, art. 132);

Chiamate senza risposta

b) è ulteriormente differito (al 31 dicembre 2009, nel caso di chiamate originate da rete mobile, e al 31 dicembre 2010, nel caso di chiamate originate da rete fissa) il termine a partire dal quale i gestori telefonici devono rendere disponibili, alla polizia e all'autorità giudiziaria, i dati di traffico telefonico relativi alle chiamate senza risposta (art. 12-*ter* del decreto-legge, inserito dalla legge di conversione).

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

Tessuti e cellule umane

- il d.lgs. 25 gennaio 2010, n. 16, recante attuazione delle Direttive n. 2006/17/CE e n. 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. A tal fine, il decreto prevede che, nel corso del prelievo dei materiali biologici o presso l'Istituto dei tessuti,

sia assegnato un codice di identificazione unico al donatore ed ai tessuti e alle cellule donati. Inoltre, si prescrive in particolare che *"il prelievo di tessuti e cellule da donatore vivente è effettuato in un contesto che ne garantisca la salute, la sicurezza e la tutela dei dati personali"*, individuando altresì le informazioni sui dati minimi relativi al donatore/ricevente che l'Istituto dei tessuti e l'organizzazione responsabile dell'applicazione sull'uomo sono tenuti a conservare per almeno trenta anni, avvalendosi di un sistema di registrazione *"adeguato e leggibile"*;

Riorganizzazione del Cnipa

- il d.lgs. 1 dicembre 2009, n. 177, recante *"Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'art. 24 della l. 18 giugno 2009, n. 69"*, che in particolare attribuisce all'Ente (ora denominato "DigitPA") le funzioni di proporre progetti in tema di amministrazione digitale; realizzare e gestire, direttamente o avvalendosi di soggetti terzi, specifici progetti in tema di amministrazione digitale ad esso assegnati e di operare come autorità di certificazione della firma digitale, essendo peraltro preposto alla tenuta di elenchi e registri nei casi previsti dall'ordinamento;

Nuovi servizi in farmacia

- il d.lgs. 3 ottobre 2009, n. 153, emanato in attuazione della delega di cui all'art. 11 della l. n. 69/2009, in materia di *"nuovi servizi erogati dalle farmacie nell'ambito del Servizio sanitario nazionale"*, in base al quale gli assistiti possano prenotare presso le farmacie prestazioni di assistenza specialistica ambulatoriale presso le strutture sanitarie pubbliche e private accreditate, e provvedere al pagamento delle relative quote di partecipazione alla spesa a carico del cittadino, nonché ritirare i referti relativi a prestazioni di assistenza specialistica ambulatoriale effettuate presso le strutture sanitarie pubbliche e private accreditate, demandandosi a un decreto, di natura non regolamentare, del Ministro del lavoro, della salute e delle politiche sociali, d'intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano, sentito il Garante, la previsione, nel rispetto delle norme del Codice, di regole tecniche e misure di sicurezza necessarie all'effettuazione delle suddette attività. Si demanda altresì a un altro decreto dello stesso Ministro, sentito anche in questo caso il Garante, la previsione,

nel rispetto delle norme del Codice, di modalità, regole tecniche e misure di sicurezza sulla base delle quali le convezioni triennali, volte a regolare il rapporto tra il Servizio sanitario nazionale e le farmacie pubbliche e private, disciplinano le modalità di ritiro, presso le farmacie, dei suddetti referti;

Contrasto del riciclaggio

- il d.lgs. 25 settembre 2009, n. 151, recante modifiche al decreto legislativo in materia di riciclaggio (d.lgs. n. 231/2007) sul cui schema non è stato richiesto alcun parere al Garante, diversamente dal precedente decreto, su cui l'Autorità si era invece pronunciata. Molte delle novelle introdotte ampliano la categoria degli obblighi informativi e il novero dei soggetti tenuti a tali doveri, così estendendo la portata del flusso informativo connesso all'adempimento della normativa antiriciclaggio. Tra le modifiche apportate si segnalano, in particolare: la ridefinizione di *"intermediari finanziari"* rilevante per le norme antiriciclaggio; la possibilità di sostituire l'attestazione necessaria all'assolvimento degli obblighi di adeguata verifica della clientela con l'invio, per via informatica, dei dati identificativi del cliente da parte dell'intermediario che ha avuto contatto diretto con il cliente stesso; la ricomprensione, tra i soggetti sottoposti alla normativa antiriciclaggio, in materia di verifica della clientela, registrazione e conservazione dei dati, anche delle agenzie di scommesse raccolte presso i *cd.* "punti fisici" (sale Bingo, ricevitorie, ecc.); l'esclusione dell'esenzione dall'obbligo di adeguata verifica della clientela in caso di *"operazioni sospette"*; l'obbligo, sancito in capo agli intermediari finanziari, di registrare e conservare per dieci anni anche le operazioni di importo inferiore a 15.000 euro; la facoltà, per gli ordini professionali, di istituire sistemi di conservazione informatica di atti e informazioni, da utilizzare, da parte degli organi istituzionalmente competenti, per indagini in materia di contrasto al terrorismo o al riciclaggio; la legittimazione della Dia, della Uif e della Guardia di finanza a chiedere informazioni "ulteriori", per l'analisi o l'approfondimento investigativo, non solo ai soggetti che hanno effettuato segnalazioni, ma anche a coloro ai quali la segnalazione è "collegata";

Sicurezza nei luoghi di lavoro

- il d.lgs. 3 agosto 2009, n. 106, recante disposizioni integrative e correttive al d.lgs. 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza

nei luoghi di lavoro, che in particolare abroga il divieto di effettuare visite mediche in fase preassuntiva e prevede che la cartella sanitaria e di rischio sia custodita da parte del medico competente secondo modalità tali da garantire il segreto professionale e, in seguito alla cessazione del rapporto di lavoro, sia conservata per almeno dieci anni da parte del datore di lavoro, nell'osservanza della normativa prevista dal Codice. Si è inoltre prevista la comunicazione al Sistema informativo nazionale per la prevenzione (Sinp) anche dei dati sugli infortuni sotto la soglia indennizzabile;

Intermediazione finanziaria

- il d.lgs. 17 luglio 2009, n. 101, recante modifiche al Testo unico delle disposizioni in materia di intermediazione finanziaria, che, tra l'altro, attribuisce alla Consob il potere di richiedere all'organismo deputato alla gestione dell'albo dei consulenti finanziari la comunicazione di dati e notizie, nonché la trasmissione di atti e documenti, con le modalità e nei termini stabiliti dalla stessa Consob. Si modifica inoltre l'art. 97, comma 4, del Testo unico, legittimando la Consob a richiedere informazioni anche nei confronti di coloro per i quali sussista un fondato sospetto che abbiano (già) svolto un'offerta al pubblico in violazione delle disposizioni di legge. Infine, si legittima la Consob all'accesso all'archivio dei rapporti con operatori finanziari di cui all'art. 7, comma 6, del d.P.R. n. 605 del 1973, che costituisce una sezione dell'anagrafe tributaria, nel quale le banche, la società Poste italiane S.p.A., gli intermediari finanziari, e ogni altro operatore finanziario sono tenuti a rilevare e a tenere in evidenza i dati identificativi, compreso il codice fiscale, di ogni soggetto che intrattenga con loro qualsiasi rapporto. Si è inoltre reintrodotta l'obbligatorietà della pubblicazione, sui mezzi di informazione su carta stampata, delle notizie rilevanti per il risparmiatore e in particolare delle informazioni "regolamentate".

L'attività svolta dal Garante

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 amministrazioni centrali e regionali

L'Agenzia autonoma per la gestione dell'albo dei segretari comunali e provinciali ha ultimato nel 2009 l'adeguamento del proprio ordinamento al sistema di garanzie previsto dal Codice per il trattamento dei dati sensibili e giudiziari.

Nel parere reso sullo schema di regolamento predisposto dall'Agenzia (*Parere* 26 novembre 2009 [doc. *web* n. 1679411]), il Garante non ha formulato alcun rilievo, riservandosi tuttavia di verificare, con autonomo procedimento, i presupposti per l'eventuale contestazione della violazione amministrativa di cui all'art. 162, comma 2-*bis*, del Codice, con riferimento ai trattamenti di dati sensibili e giudiziari effettuati dall'Agenzia in assenza del regolamento previsto dall'art. 20 del Codice, il quale doveva essere emanato entro il 28 febbraio 2007 (art. 181 del Codice, come modificato dal comma 1 dell'art. 6, del d.l. 28 dicembre 2006, n. 300, conv. con l. 26 febbraio 2007, n. 17).

3.1.2. I regolamenti degli enti locali

Nell'anno di riferimento, si è registrato un significativo decremento di richieste di pareri degli enti locali relativamente a trattamenti di dati sensibili o giudiziari ritenuti non ricompresi, per tipologia di dati o di operazioni, né negli schemi tipo di regolamento sui quali il Garante si è espresso favorevolmente (*cfr.* schemi Anci-Associazione nazionale dei comuni italiani [doc. *web* n. 1174532], Upi-Unione delle province d'Italia [doc. *web* n. 1174562] e Uncem-Unione nazionale comuni comunità enti montani [doc. *web* n. 1182195], *cfr. Relazione 2006*, p. 19), né nei pareri con i quali il Garante si è espresso positivamente con riferimento a ulteriori trattamenti di dati sensibili e giudiziari non considerati nei predetti schemi tipo (*cfr. Relazione 2005*, p. 20 [doc. *web* n. 1213424]; *cfr. Relazione 2006*, pp. 34 e 35 [doc. *web* nn. 1213424, 1298732, 1314392, 1370369,

1377640, 1434995]; *cfr. Relazione 2008*, p. 51 [doc. *web* n. 1507195]).

Tra i casi maggiormente significativi si segnalano le richieste di un consorzio di comuni in ordine ad una integrazione del proprio statuto, volta a consentire ai comuni aderenti il trattamento di taluni tipi di dati sensibili per la rendicontazione ed il monitoraggio della spesa dei servizi socio-assistenziali. In proposito, è stato evidenziato che il consorzio stesso è tenuto a verificare che il trattamento da effettuare sia disciplinato da un'espressa disposizione di legge - nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite - ovvero da un atto di natura regolamentare adottato in conformità allo schema tipo Anci. In ogni caso, i soggetti pubblici possono trattare solo i dati sensibili indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa (art. 22, comma 3, del Codice) (*Nota* 22 giugno 2009).

Una provincia aveva chiesto al Garante un parere riguardo alla necessità di effettuare talune operazioni non ricomprese nel citato schema tipo Upi, in particolare di interconnessione e raffronto di dati sensibili con banche dati di altri titolari del trattamento nel quadro delle attività finalizzate al collocamento e all'avviamento al lavoro (art. 73, comma 2, lett. *i*), del Codice) e alla cura dell'integrazione sociale, nonché del collocamento obbligatorio nei casi previsti dalla legge (art. 86, comma 1, lett. *c*), n. 2, del Codice). E' stato rappresentato che le predette operazioni rientrano tra quelle che possono spiegare effetti maggiormente significativi per gli interessati e, quindi, devono essere sia delimitate rigorosamente in conformità al principio di indispensabilità, sia previste espressamente per legge qualora comportino un possibile raffronto tra dati sensibili detenuti da distinti titolari del trattamento (art. 22, commi 10 e 11 del Codice). Nell'ambito delle predette attività si ritengono leciti unicamente l'interconnessione e il raffronto con comuni della provincia per il coordinamento degli sportelli anagrafe del lavoro e degli sportelli decentrati (*cfr.* d.lgs. 23 dicembre 1997, n. 469), nonché con regione ed operatori pubblici e privati accreditati o autorizzati nell'ambito della Borsa continua nazionale del lavoro (*cfr.* d.lgs. 10 settembre 2003, n. 276) limitatamente alle informazioni indispensabili

all'instaurazione di un rapporto di lavoro, come individuate nello schema-tipo Upi. E' stato infine ricordato che il Garante, nel *parere* del 18 maggio 2006 [doc. *web* n. 1434995], si era espresso in senso favorevole in ordine alle interconnessioni finalizzate al perseguimento della finalità di rilevante interesse pubblico di cui al citato art. 73, comma 1, lett. *b*), del Codice, ai soli fini dell'accertamento d'ufficio di stati, qualità e fatti, ovvero del controllo su dichiarazioni sostitutive prodotte dagli interessati (*v.* art. 43 d.P.R. 28 dicembre 2000, n. 445) (*Nota* 1° settembre 2009).

Un istituto case autonome popolari aveva chiesto se vi fosse uno schema-tipo di regolamento per il trattamento dei dati sensibili e giudiziari, cui poter fare riferimento. Al riguardo, è stato sottolineato che la Conferenza delle Regioni e delle Province autonome ha adottato uno schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali, nonché degli enti vigilati dalle regioni e dalle province autonome, sul quale il Garante ha espresso parere favorevole [doc. *web* n. 1272225]. Tale documento costituisce lo schema-tipo in conformità al quale può essere adottato da parte dell'amministrazione regionale l'atto regolamentare volto a disciplinare i trattamenti effettuati anche dagli enti vigilati da tale amministrazione. L'istituto, quale ente strumentale, è tenuto a rispettare le specifiche disposizioni che lo riguardano contenute nel regolamento adottato dalla regione, senza dover chiedere un ulteriore parere formale dell'Autorità, ai sensi dell'art. 20, comma 2, del Codice (*Nota* 22 febbraio 2010).

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

Come già negli anni precedenti (*cfr. Relazione 2008*, p. 51) sono pervenute diverse richieste di intervento del Garante nei confronti di amministrazioni pubbliche che hanno respinto richieste di accesso presentate ai sensi della l. 7 agosto 1990, n. 241. Se ne dà conto, di seguito, evidenziando i profili in fatto che caratterizzano la casistica in esame.

A fronte di una richiesta di autorizzazione rivolta al Garante al fine di ottenere taluni

dati personali, riguardanti il padre biologico della richiedente, detenuti da un comando regionale dei Carabinieri, l'Ufficio ha evidenziato che la questione esula dalla competenza dell'Autorità, e riguarda più direttamente la normativa sull'accesso ai documenti amministrativi, non abrogata dal Codice (artt. 59 e 60); le scelte dell'amministrazione interpellata non sono sindacabili dinanzi all'Autorità, bensì innanzi alle autorità competenti (art. 25, l. n. 241/1990, come modificata dalla l. n. 15/2005 *cit.*) (*Nota* 3 novembre 2009).

Analoghe considerazioni sono state formulate relativamente ad una richiesta volta ad ottenere un'autorizzazione del Garante al fine di vedere soddisfatta un'istanza di accesso a un prospetto oneri Inail, corredato dalla rendita con i valori capitali aggiornati del danno biologico e patrimoniale, per confutare la pretesa risarcitoria della parte avversa al richiedente, nell'ambito di un procedimento giudiziario di risarcimento per danni sofferti a seguito di un sinistro stradale. Al riguardo è stato in particolare evidenziato che laddove gli atti richiesti contengano informazioni idonee a rivelare lo stato di salute o la vita sessuale dell'interessato, occorre previamente valutare il *"rango"* del diritto dedotto dal richiedente, il quale deve essere *"almeno pari"* rispetto ai diritti dell'istante, ovvero consistere in un diritto della personalità o in altro diritto o libertà fondamentale e individuale (art. 60 del Codice, *cfr. provvedimento* del 9 luglio 2003, *Relazione 2003*, p. 65 [doc. *web* n. 29832]) (*Nota* 20 maggio 2009).

Ad un soggetto che aveva chiesto l'intervento dell'Ufficio, al fine di vedere soddisfatta una richiesta di cancellazione dei dati personali che lo riguardavano dal sito *web* di un comune, nonché per l'annullamento della delibera che li conteneva, è stato fatto presente che l'annullamento degli atti adottati dalle amministrazioni pubbliche esula dall'ambito di competenza del Garante. Solo in caso di mancato, parziale o inidoneo riscontro del titolare del trattamento alla richiesta di accesso ai dati personali esercitata ai sensi dell'art. 7 del Codice medesimo, l'interessato può rivolgersi all'autorità giudiziaria o presentare formale ricorso al Garante, secondo le modalità previste dal Codice (art. 145) (*Nota* 20 aprile 2009).

I quesiti, le segnalazioni ed i reclami inerenti la pubblicazione di atti e documenti

contenenti dati personali hanno impegnato il Garante in diverse occasioni.

In relazione ad un quesito riguardante la pubblicazione sul sito *web* del Senato della Repubblica di dati personali riportati in un atto di sindacato ispettivo, è stato chiarito che la diffusione di dati personali da parte dei soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento (art. 19, comma 3, del Codice). In tale quadro, il regolamento del Senato garantisce espressamente la pubblicità degli atti e delle sedute dell'Assemblea prevedendo, in particolare, che *"di ogni seduta pubblica vengono redatti e pubblicati il resoconto sommario ed il resoconto stenografico"* (*Nota* 25 marzo 2009).

Con apposite *"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], in *G.U.* 25 maggio 2007, n. 120; *Relazione 2007*, p. 40), il Garante si è pronunciato relativamente a molteplici e controversi casi di diffusione di dati personali da parte di soggetti pubblici, per dare pubblicità all'attività istituzionale, specie tramite tecniche informatiche e telematiche.

In una segnalazione si era lamentata la diffusione sul sito *web* di un comune di delibere adottate dalla giunta comunale, dalle quali emergevano dati particolarmente delicati riguardanti la difficile situazione familiare e finanziaria della segnalante e del figlio minore. Nel chiedere al Comune chiarimenti in proposito, l'Ufficio ha evidenziato che, sulla base delle citate linee-guida, sono divulgabili - per periodi di tempo congrui, rispetto alle finalità perseguite, specie nel caso della diffusione in internet - solo i dati personali necessari per rendere conoscibile la delibera con la quale si attribuiscono determinati benefici; tra tali informazioni non sono ricompresi il punteggio Isee, le situazioni di particolare disagio o di bisogno ovvero le peculiari situazioni abitative, fermo restando il divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (artt. 22, comma 8, 65, comma 5, e 68, comma 3, del Codice). Poiché il sindaco aveva dichiarato di aver immediatamente provveduto a rimuovere dal sito *web* istituzionale le delibere in questione, non sono stati adottati 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* 24 luglio 2009).

A seguito della pubblicazione sul sito *web* di un comune dell'elenco dei soggetti ai quali

erano stati erogati contributi economici integrativi della retta scolastica, era stato chiesto l'intervento dell'Autorità al fine di vedere cancellate talune informazioni contenute nella predetta lista, in particolare le generalità del minore affidato alla segnalante medesima ed il relativo indirizzo. Dagli accertamenti preliminari dell'Ufficio, tramite l'inserimento del nominativo del beneficiario nei più diffusi motori di ricerca, è emerso che nella versione *HTML* della pagina *web* istituzionale risultava ancora visibile l'intera graduatoria e che, inoltre, l'*abstract* dell'esito della ricerca nei motori di ricerca esterni riportava le generalità del suddetto beneficiario, nonché il relativo indirizzo. Alla luce dei princìpi enucleati nelle citate linee-guida, il comune è stato invitato ad impedire la consultazione dei contenuti delle predette pagine *web* e la relativa indicizzazione da parte dei principali motori di ricerca. Poiché l'amministrazione comunale in questione ha provveduto a correggere l'errore, intervenendo sia sulle pagine *web* di propria competenza, sia sui motori di ricerca esterni, non sono state adottate ulteriori misure nei suoi confronti (artt. 11, comma 1, lett. *d*), e 13, comma 4, del *Regolamento* del Garante n. 1/2007) (*Nota* 3 novembre 2009).

In due casi analoghi, da notizie di stampa era emerso che nel sito *web* di due diversi comuni risultavano consultabili gli albi dei beneficiari di provvidenze di natura economica recanti, in corrispondenza di taluni nominativi, il riferimento normativo in base al quale soggetti portatori di *handicap* possono fruire di benefici e titoli di preferenza, in violazione del divieto, richiamato nelle linee-guida *cit.*, di diffondere dati idonei a rivelare lo stato di salute degli interessati (art. 22, comma 8, del Codice). Inoltre, sulla base degli accertamenti preliminari effettuati, i suddetti elenchi erano risultati visualizzabili anche tramite l'inserimento del nominativo dei beneficiari nei più diffusi motori di ricerca. Entrambi i comuni, opportunamente richiamati al rispetto delle predette disposizioni, hanno eliminato i riferimenti idonei a rivelare lo stato di salute ed escluso dall'indicizzazione il *file* riferito all'albo, il quale è stato reso raggiungibile esclusivamente attraverso i collegamenti interni del sito (*Note* 4 novembre 2009 e 16 febbraio 2010).

Alcuni consiglieri comunali di minoranza avevano lamentato la pubblicazione sul sito dell'amministrazione di riferimento di una deliberazione in cui erano riportate, in forma estesa e senza *omissis*, le generalità di un cittadino in stato vegetativo al quale veniva finan-

ziato il ricovero in una casa di cura nonché il nome e cognome del padre che contribuiva al pagamento della retta. I segnalanti avevano evidenziato, inoltre, che in un'altra delibera, sempre visibile sul sito del medesimo ente, erano riportate le generalità anche di altri cittadini indigenti, destinatari di fondi stanziati dall'amministrazione per la loro permanenza in una casa di riposo.

L'Autorità ha vietato la diffusione dei dati idonei a rivelare lo stato di salute contenuti nella prima delibera, ritenendo il trattamento illecito e sottolineando che le amministrazioni locali devono selezionare attentamente i dati personali oggetto di diffusione, alla luce dei princìpi di pertinenza, non eccedenza e indispensabilità delle finalità perseguite nonché del divieto di diffusione di dati idonei a rivelare lo stato di salute (artt. 11, comma 1, lett. *d)*, 22, commi 3 ed 8, del Codice). L'Autorità ha prescritto al comune di sollecitare, ai responsabili dei principali motori di ricerca esterni, la rimozione della copia *web* della prima delibera dai loro indici e memorie *cache*. All'ente è stato prescritto, infine, di adottare opportuni accorgimenti (diciture generiche o codici numerici) atti ad evitare che sulla seconda delibera, consultabile sul sito, fossero presenti dati sulle condizioni sociali disagiate degli anziani citati (*Provv.* 7 ottobre 2009 [doc. *web* n. 1664456]).

In un altro caso era stata lamentata la pubblicazione sul sito *web* di una università della graduatoria di ammissione dei candidati ad un corso di studi. Nel richiedere informazioni sulla vicenda, l'Ufficio ha sottolineato che se la finalità da perseguire riguarda prevalentemente solo alcune categorie di persone, devono essere previste forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*, numero di protocollo o altri estremi identificativi di una pratica forniti dall'ente agli aventi diritto), comunque sempre nel rispetto dei predetti princìpi di pertinenza e non eccedenza. Poiché l'università ha rimosso la graduatoria dal sito accademico, non sono state intraprese iniziative per l'adozione di specifici provvedimenti da parte del Garante (artt. 11, comma 1, lett. *d*), e 13, comma 4, del *Regolamento* del Garante n. 1/2007) (*Nota* 19 gennaio 2010).

Anche le problematiche legate al diritto dei consiglieri comunali e provinciali di accedere agli atti dell'ente di riferimento sono state oggetto di esame in diverse occasioni.

Era stato chiesto se la diffusione del contenuto di atti, di cui i consiglieri comunali siano entrati in possesso per l'esercizio del loro mandato, tramite siti *web* privati, fosse conforme al Codice. Sul punto è stato ricordato che i consiglieri comunali, pur avendo diritto di accesso agli atti del comune, sono tenuti a rispettare il dovere di segreto *"nei casi specificamente determinati dalla legge"* (art. 43 del d.lgs. 18 agosto 2000, n. 267) e ad osservare i divieti di divulgazione dei dati personali (art. 22, comma 8, del Codice), nonché i princìpi di liceità, finalità, pertinenza e non eccedenza del trattamento (art. 11, comma 1, lett. *a*), *b*), e *d*), del Codice). Considerato, altresì, che tutte le deliberazioni del comune e della provincia sono conoscibili da chiunque (art. 124 d.lgs. n. 267/2000 *cit.*), si è ritenuto che i princìpi contenuti nelle citate linee-guida, pur non attinenti direttamente ai trattamenti posti in essere nei siti *web* privati, devono comunque essere tenuti presenti da questi ultimi quando si intenda in essi ripubblicare o diffondere dati personali contenuti nei suddetti atti.

E' stato osservato, inoltre, che specifiche disposizioni estendono l'ambito applicativo delle norme concernenti il trattamento dei dati personali in ambito giornalistico ad altre attività di manifestazione del pensiero svolte da soggetti che non esercitano professionalmente l'attività giornalistica (art. 136, comma 1, lett. *c*), del Codice). In tale contesto, possono pertanto essere diffusi dati personali, anche senza il consenso degli interessati, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; art. 6 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, Allegato A.1. del Codice) (*Nota* 19 maggio 2009).

Una società, che cura *"in house"* la riscossione volontaria e coattiva delle entrate per conto di un comune, aveva formulato un quesito sulla possibilità di rendere ostensibili taluni documenti ad un consigliere comunale che ne aveva fatto richiesta ai sensi dell'art. 43 del d.lgs. n. 267/2000 *cit.*. In proposito, poiché la protezione dei dati personali non pregiudica l'applicazione della normativa sulla trasparenza, è stato rappresentato che spetta alla società, in relazione allo specifico rapporto *"in house"* con l'amministrazione comunale, quale destinataria della richiesta di accesso, accertare l'ampia e qualificata

posizione di pretesa all'informazione *ratione officii* del consigliere comunale e individuare le modalità per assolvere a tale richiesta (*Nota* 27 novembre 2009).

Un comune aveva formulato un quesito in ordine alla possibilità di rendere ostensibile ad un proprio consigliere comunale, i contenuti della corrispondenza intercorsa per via telematica tra un dipendente comunale ed un consulente esterno. E' stato osservato che il citato art. 43, comma 2, d.lgs. n. 267/2000 *cit.* deve essere coordinato con altre norme vigenti che tutelano, in particolare, la segretezza della corrispondenza e delle conversazioni. Ciò in considerazione della natura particolarmente delicata dei dati contenuti nei messaggi di posta elettronica, la cui utilizzazione impropria può avere ripercussioni sulla sfera personale di più soggetti interessati (il mittente e il ricevente).

Più in particolare, il Garante, nelle *"Linee-guida per posta elettronica e internet"* del 1° marzo 2007 (in *G.U.* 10 marzo 2007 n. 58 [doc. *web* n. 1387522]), aveva evidenziato come il contenuto dei messaggi di posta elettronica, i dati esteriori delle comunicazioni ed i *file* allegati costituiscono forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, comma 4, c.p.; art. 49 codice dell'amministrazione digitale) (*par.* 5.2.*b* del *provvedimento cit.*). E' stato perciò fatto presente che il trattamento dei dati personali oggetto della richiesta di accesso in questione deve essere effettuato in conformità al citato quadro normativo (*Nota* 23 febbraio 2010).

Sotto un diverso profilo, un comune aveva chiesto il parere dell'Ufficio in ordine a talune disposizioni del proprio regolamento riguardanti la registrazione, anche da parte di organi di informazione, delle sedute del consiglio comunale. Al riguardo, premesso che il Garante esprime pareri esclusivamente nei casi previsti, nonché qualora il Presidente del Consiglio dei ministri e ciascun ministro predispongano norme regolamentari ed atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice (art. 154, commi 1, lett. *g*), e 4, del Codice) è stato rappresentato che non sussistono ostacoli

di fondo all'effettuazione di registrazioni delle sedute del consiglio comunale, in quanto i soggetti pubblici possono trattare dati personali unicamente per lo svolgimento delle proprie funzioni istituzionali, nel rispetto dei presupposti e dei limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti (artt. 18, commi 2 e 3, e 19, comma 1). In tale quadro, il Testo unico delle leggi sull'ordinamento degli enti locali stabilisce espressamente che le sedute del consiglio e delle commissioni sono pubbliche, salvi i casi previsti dal regolamento; pertanto, è stata ricordata all'amministrazione comunale la sua competenza ad introdurre eventuali limiti a detto regime di pubblicità, mediante un atto di natura regolamentare (art. 38 del d.lgs. n. 267/2000 *cit.*), non essendo previsto che tali scelte, effettuate in attuazione del citato d.lgs., siano oggetto di esame preliminare da parte del Garante. Ciò fermo restando l'obbligo di rendere l'informativa agli interessati attraverso l'affissione di avvisi chiari e sintetici, circa l'esistenza di strumenti radiotelevisivi e la successiva diffusione delle immagini o dei discorsi (art. 13 del Codice) (*Nota* 10 novembre 2009).

3.3. LA DOCUMENTAZIONE ANAGRAFICA E LA MATERIA ELETTORALE

Numerose problematiche riguardanti il corretto trattamento dei dati personali sono emerse nel quadro della gestione dei servizi demografici in ambito comunale.

Erano stati chiesti chiarimenti in ordine alla possibilità di soddisfare la richiesta, presentata dagli eredi del defunto, di ottenere copia dell'atto di un matrimonio celebrato in costanza di imminente pericolo di vita di uno dei due nubendi, nonché di accedere ai relativi allegati, compreso il certificato medico attestante le sue gravi condizioni di salute.

Nel rappresentare che il Codice non ha modificato espressamente né la disciplina vigente in materia di stato civile e anagrafe (*cfr.* r.d. 9 luglio 1939 n. 1238; art. 450 c.c.; l. 24 dicembre 1954, n. 1228; d.P.R. 30 maggio 1989, n. 223; l. 15 maggio 1997, n. 127; d.P.R. 3 novembre 2000, n. 396), né le norme vigenti in materia di accesso ai documenti amministrativi (artt. 22 *ss.*, l. n. 241/1990, così come modificata dalla l. n. 15/2005 *cit.*; art. 2 d.P.R. n. 184/2006 *cit.*), è stato fatto presente che nelle predette ipotesi, spetta all'amministrazione destinataria della richiesta di accesso verificare,

caso per caso, l'interesse e i motivi sottesi alla relativa istanza, nonché valutare la sussistenza di una delle ragioni per le quali il documento può essere sottratto alla conoscibilità del richiedente (*Nota* 24 aprile 2009).

Ad un comune che aveva chiesto se fosse possibile abilitare i centri di assistenza fiscale alla visualizzazione diretta dei dati anagrafici mediante un *software* che consente con collegamento *web* di accedere ad una copia dell'anagrafe comunale aggiornata al giorno precedente, l'Ufficio ha ricordato che, con il *provvedimento* del 6 ottobre 2005 (in *G.U.* 2 ottobre 2005, n. 248 [doc. *web* n. 1179484]; *Relazione 2005*, p. 30), è stato già evidenziato come, ad eccezione del personale autorizzato delle forze di polizia, i dati contenuti nell'anagrafe della popolazione residente non possono essere consultati direttamente da parte di chiunque, anche facente parte del personale comunale, sia estraneo all'ufficio di anagrafe. I comuni possono attivare un flusso di dati anagrafici su richiesta, anche con strumenti automatizzati e per via telematica, per finalità di snellimento ed efficienza dell'azione amministrativa, prevedendo che le richieste di certificazione o attestazione, oppure di rilascio di elenchi ad amministrazioni pubbliche, motivato da ragioni accertate di pubblica utilità, possano essere inoltrate e riscontrate anche automaticamente, per via telematica, escludendo però la consultazione diretta, anche *online*, degli atti di provenienza anagrafica da parte di soggetti diversi da quelli preposti all'ufficio anagrafe (*Nota* 24 aprile 2009).

Analoghe considerazioni sono state formulate con riferimento ad un comune che aveva inoltrato per opportuni chiarimenti, le richieste di un comando provinciale della Guardia di finanza e di un comando provinciale della Legione Carabinieri finalizzate a consentire, tramite convenzione, l'accesso all'anagrafe della popolazione residente. Al riguardo è stato rilevato che la disciplina di settore prevede espressamente la consultazione degli atti anagrafici da parte degli appartenenti alle forze dell'ordine, consentendo a queste ultime di accedere all'ufficio di anagrafe e di consultare direttamente gli atti anagrafici. All'ufficiale dell'anagrafe devono essere comunicati gli estremi del personale abilitato alla consultazione, il quale deve operare secondo modalità tecniche adottate d'intesa tra gli uffici anagrafici comunali e gli organi interessati (art. 37, commi 1 e 4, d.P.R. n. 223/1989 *cit.*).

In tale quadro è stato ricordato che il Garante, con il citato *provvedimento* del 6 ottobre 2005, aveva evidenziato che le predette disposizioni riguardano il particolare contesto degli atti anagrafici, i quali giustificano soluzioni specifiche per quanto riguarda le modalità della loro consultazione, anche mediante flussi di dati, trasmissioni o consultazioni telematiche di dati ed archivi (art. 2, comma 5, l. n. 127/1997 *cit.*; art. 43 d.P.R. n. 445/2000 *cit.*) (*Nota* 19 gennaio 2010).

Sono state chieste delucidazioni in ordine alla trasmissibilità di elenchi dei dati anagrafici all'Agenzia delle entrate di Torino-Sportello abbonamenti alla televisione. Nel ricordare che la comunicazione di dati personali ad altri soggetti pubblici è ammessa quando sia espressamente prevista da norme di legge o di regolamento, o risulti, comunque necessaria per lo svolgimento delle funzioni istituzionali (art. 19, comma 2, del Codice), è stato osservato che la disciplina sugli atti anagrafici prevede la possibilità per l'ufficiale dell'anagrafe di rilasciare (anche periodicamente) elenchi di iscritti nell'anagrafe della popolazione residente esclusivamente ad amministrazioni pubbliche che ne facciano motivata richiesta, *"per esclusivo uso di pubblica utilità"* (art. 34, comma 1, d.P.R. n. 223/1989 *cit.*) (*Nota* 24 giugno 2009).

In un caso diverso, un comune aveva formulato un quesito in ordine alla trasmissibilità periodica tramite posta elettronica, ad una Asl, di dati contenuti nell'anagrafe della popolazione residente. Fermo restando quanto previsto dal citato d.P.R. n. 223/1989 in ordine alla comunicazione di elenchi anagrafici a soggetti pubblici, è stato osservato che la posta elettronica ordinaria non è mezzo idoneo per la trasmissione dei dati alla Asl, in quanto non è in grado di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (artt. 31 *ss.* del Codice). Inoltre, la posta elettronica ordinaria, diversamente dalla posta elettronica certificata, non è in grado di documentare l'avvenuta spedizione e ricezione dei messaggi (*Nota* 23 febbraio 2010).

Il Garante ha accolto l'invito dell'Anci a partecipare ad un tavolo di lavoro dedicato all'integrazione e alla circolarità anagrafica, temi ricompresi tra gli obiettivi del *"Piano e-gov 2012"* sia del Ministero per la pubblica amministrazione e l'innovazione,

sia delle regioni, che li hanno inseriti tra le priorità dei prossimi progetti interregionali siglando un protocollo di intesa in merito con il Ministero dell'interno (*Nota* 7 maggio 2009).

Un ateneo si era rivolto al Garante chiedendo se fosse ammissibile il rilascio di un nuovo diploma sia di laurea, sia di specializzazione, all'interessato che ne aveva fatto richiesta a seguito di un percorso medico legale di riattribuzione del sesso. Sul punto, richiamata la possibilità di ottenere la rettificazione degli atti dello stato civile a seguito di una sentenza del tribunale passata in giudicato, che attribuisca alla persona sesso diverso da quello enunciato nell'atto di nascita (art. 2, comma 5, l. 14 aprile 1982, n. 164), è stato ricordato il diritto dell'interessato di ottenere, rivolgendosi direttamente al titolare del trattamento (nella specie l'ateneo), l'aggiornamento o la rettificazione dei dati che lo riguardano (art. 7, comma 3, lett. *a*), del Codice) (*Nota* 7 aprile 2009).

Sotto un diverso profilo, una cittadina aveva lamentato che i riferimenti allo stato civile (coniugio o vedovanza) delle donne non nubili contenuti sia nelle liste elettorali, sia nella tessera elettorale, comportano una presunta violazione della riservatezza. Al riguardo è stato evidenziato che le indicazioni di tali dati in applicazione della normativa di settore non costituisce violazione del Codice (*Nota* 30 giugno 2009).

3.4. L'ISTRUZIONE

3.4.1. La scuola

Durante l'anno di riferimento il Garante si è espresso più volte in materia di trattamento dei dati personali in ambito scolastico.

L'Ufficio ha avuto occasione di fornire chiarimenti al genitore di uno studente minore in relazione alle corrette modalità di utilizzo di materiale fotografico ed audiovisivo da parte delle istituzioni scolastiche.

Al riguardo, richiamata la direttiva n. 104 del Ministero della pubblica istruzione (recante linee di indirizzo e chiarimenti interpretativi con particolare riferimento all'utilizzo di telefoni cellulari o altri dispositivi elettronici nelle comunità scolastiche), emanata il 30 novembre 2007, con *parere* favorevole del Garante [doc. *web* n. 1466996],

l'Ufficio non ha ravvisato alcuna violazione del Codice, anche in considerazione del fatto che la scuola aveva dichiarato di avere acquisito il consenso della madre della minore ad utilizzare per puro uso interno, le immagini della bambina raccolte durante manifestazioni scolastiche (*Nota* 30 gennaio 2009).

Il Ministero dell'istruzione dell'università e della ricerca aveva posto un quesito all'Autorità sulla pubblicazione dei risultati degli esami conclusivi dei corsi di studio di istruzione secondaria di secondo grado. In particolare, era stato chiesto se le indicazioni, fornite con la nota del 20 giugno 2008 (prot. n. 7017) Dipartimento per l'istruzione del Ministero, sulla corretta attuazione dell'art. 21 dell'ordinanza ministeriale 10 marzo 2008, n. 30, fossero conformi alla normativa in materia di protezione dei dati personali.

La disposizione in questione prevede che l'esito degli esami di Stato, conclusivi dei corsi di studio di istruzione secondaria superiore nelle scuole statali e non statali, sia pubblicato, per tutti i candidati, nell'albo dell'istituto sede della commissione, con la sola indicazione della dizione "diplomato", o "non diplomato", indicando altresì l'eventuale attribuzione della lode. Nella medesima ordinanza è previsto che il riferimento dell'effettuazione delle prove differenziate, che vengono sostenute da allievi portatori di *handicap*, va indicato solo nell'attestazione e non anche nei tabelloni affissi all'albo. Il Dipartimento per l'istruzione del Ministero aveva temuto che tale disciplina potesse determinare una ingiustificata disparità di trattamento degli allievi disabili, non potendo questi, a seguito della prova differenziata, comparire nell'albo dell'istituto, nè ottenere la qualifica di "diplomato" o "non diplomato".

Alla luce di queste considerazioni il Dipartimento per l'istruzione del Ministero aveva disposto che, presso l'albo dell'istituto sede della commissione, venisse pubblicato l'elenco di tutti i candidati - compresi i portatori di *handicap* - con la sola indicazione *"esito positivo"* o *"esito negativo"*, facendo altresì menzione dell'eventuale attribuzione della lode.

L'Autorità ha ritenuto che la citata soluzione applicativa dell'art. 21 riesca a valorizzare non solo la tutela degli interessi degli alunni disabili, ma anche le esigenze di trasparenza degli esiti finali degli esami di Stato, e pertanto, anche in considerazione dell'art. 96,

comma 2 del Codice - che fa salva la disciplina in materia di pubblicazione dell'esito degli esami - non ha formulato alcuna osservazione in merito (*Nota* 31 marzo 2009).

Nel periodo di riferimento l'Autorità ha collaborato con il Ministero dell'istruzione dell'università e della ricerca in merito allo schema di decreto in corso di predisposizione per la realizzazione dell'anagrafe nazionale degli studenti.

Con tale strumento si intende favorire la realizzazione del diritto-dovere all'istruzione ed alla formazione, nonché vigilare sull'assolvimento dell'obbligo scolastico. A tal fine, le istituzioni scolastiche, anche non statali e non paritarie, dovranno comunicare all'anagrafe alcune informazioni relative ai percorsi scolastici, formativi ed in apprendistato, dei singoli studenti a partire dal primo anno della scuola primaria.

Per garantire l'interesse del minore al rispetto alla sua vita privata, il Garante ha fornito alcune indicazioni affinché il Ministero raccolga dati non eccedenti, proporzionali e pertinenti rispetto alle finalità amministrative che, nell'ambito delle proprie competenze, intende perseguire, anche nell'ottica di prevenire eventuali discriminazioni (art. 11 del Codice). L'Autorità ha, inoltre, rammentato che per il trattamento dei dati sensibili e giudiziari vanno rispettate le specifiche garanzie approntate dal Codice, richiamando in particolare il principio di indispensabilità (artt. 20 e 22 del Codice).

Il Garante ha, inoltre, rappresentato la necessità di salvaguardare il diritto all'oblio dei minori, prestando attenzione ai tempi di conservazione dei dati che possono rapidamente diventare obsoleti rispetto alle finalità iniziali della raccolta.

3.4.2. L'università

L'Autorità ha altresì fornito alcuni chiarimenti alle università sulle corrette modalità di trattamento dei dati personali relativi agli studenti.

In particolare, un'università aveva chiesto al Garante se fosse possibile comunicare ad un giornalista l'elenco dei laureati negli ultimi due anni che hanno avuto il riconoscimento di sessanta crediti. Al riguardo, il Codice consente ai soggetti pubblici, quali le università, di comunicare dati personali diversi da quelli sensibili a soggetti privati solo se previsto da una norma di legge o di regolamento (art. 19, comma 3, del Codice).

L'Ufficio, rilevata l'assenza di tale specifica norma, ha, tuttavia, evidenziato, in primo luogo, che ciascuna università, nell'ambito della propria autonomia regolamentare, può disciplinare il regime di conoscibilità dei dati riguardanti i laureati.

In secondo luogo, è stato rappresentato che il Codice prevede che i soggetti pubblici, ivi compresi le università e gli enti di ricerca, possono comunicare, con autonome determinazioni, e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e ricerca, con esclusione di quelli sensibili, a laureati, ricercatori, docenti, al solo fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico (art. 100 del Codice) (*Nota* 21 gennaio 2009).

Infine, merita menzione la vicenda relativa alla presunta illecita diffusione di dati personali da parte del Ministero dell'istruzione, dell'università e della ricerca tramite l'anagrafe nazionale degli studenti.

L'Ufficio, ha, infatti, avuto modo di verificare le funzionalità del motore di ricerca dell'Osservatorio "Anagrafe studenti".

In particolare, è stato riscontrato che attraverso le maschere "Anagrafe nazionale studenti" e "Ricerca avanzata" possono effettuarsi interrogazioni che restituiscono informazioni su persone fisiche e giuridiche identificate o identificabili, indirettamente con l'impiego di mezzi ragionevoli, mediante il riferimento ad altre informazioni (*cfr.* art. 4, comma 1, lett. *b*), del Codice; artt. 3 e 4 del codice di deontologia e buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistan).

Successivamente, è stato verificato che il Ministero stesso aveva, per autotutela, bloccato gli accessi al sito internet relativo all'Osservatorio "Anagrafe studenti", al fine di consentire l'adeguamento a quanto previsto dagli articoli 3 e 4 del predetto codice di deontologia (*Nota* 2 gennaio 2009).

3.5. ATTIVITÀ FISCALE, TRIBUTARIA E DOGANALE

Anche nel 2009 il Garante ha proseguito l'attività di controllo sui trattamenti di dati personali effettuati nell'ambito dell'attività fiscale e tributaria.

Come indicato nel *provvedimento* del 18 settembre 2008 (*cfr. Relazione 2008*, p. 70 [doc. *web* n. 1549548]), il Garante aveva prescritto all'Agenzia delle entrate l'adozione di un'articolata serie di misure, tecnologiche e organizzative, per innalzare i livelli di sicurezza degli accessi all'anagrafe tributaria da parte degli enti esterni e rendere il trattamento dei dati conforme alla normativa. Tuttavia, nel 2009, l'Agenzia ha richiesto al Garante numerose proroghe dei termini inizialmente previsti, in considerazione della complessità delle misure da adottare e dell'elevato numero dei soggetti coinvolti, soprattutto con riferimento ai comuni.

Con il *provvedimento* del 26 marzo 2009 [doc. *web* n. 1605576], su richiesta dell'Agenzia delle entrate, il Garante ha prorogato i termini per alcune prescrizioni ma, considerati i lunghi tempi prospettati, in particolare, per la verifica dei presupposti giuridici di accesso all'anagrafe tributaria da parte degli enti esterni, ha previsto che:

1) gli enti, attraverso i propri amministratori locali (deputati alla gestione delle utenze), accertino, sotto la propria responsabilità, l'attualità di ciascuna utenza attiva, anche in relazione alle finalità per cui è stata attribuita, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni, fornendo riscontro, anche telematico, di tale verifica, all'Agenzia entro il 30 giugno 2009;
2) l'Agenzia, in mancanza del suddetto riscontro, a partire dal 1° ed entro il 31 luglio 2009, disattivi tutte le utenze degli enti diverse da quelle in uso agli amministratori locali, avvisando gli enti medesimi che, prima di procedere all'eventuale riattivazione degli utenti attraverso i propri amministratori locali, dovranno effettuare, sotto la propria responsabilità, la verifica di cui al punto precedente.

Con *provvedimento* 24 settembre 2009 [doc. *web* n. 1657692], per alcuni enti (Inps, Inpdap, Enpals, Avcp, camere di commercio e Agea) è stata prorogata al 30 novembre 2009 l'adozione degli adempimenti relativi alla dismissione dei *web services* e del collegamento denominato *"3270 enti esterni"*, già prorogati al 30 settembre 2009

con i *provvedimenti* del 2 luglio 2009 [doc. *web* n. 1640373], 17 luglio 2009 [doc. *web* n. 1639318] e 23 luglio 2009 [doc. *web* n. 1640317 e doc. *web* n. 1640349]; è stato inoltre prorogato il termine per alcuni adempimenti prescritti con il citato *provvedimento* del 26 marzo 2009 sugli accessi da parte dei comuni: al termine di tale periodo gli accessi all'anagrafe tributaria devono avvenire unicamente con procedure idonee a offrire le garanzie già indicate dal Garante nel citato *provvedimento* del 18 settembre 2008.

In seguito, l'Agenzia delle entrate ha illustrato al Garante alcune caratteristiche relative ad una nuova classe di *web services* in fase di sperimentazione, che offre un accesso ai dati personali più ampio rispetto a quello già individuato dall'Autorità nel citato *provvedimento* 2008, trasmettendo anche il corrispondente modello di convenzione volto a regolare le condizioni d'uso e gli obblighi in materia di protezione dei dati personali.

Il Garante ha quindi ritenuto necessario valutare la conformità al Codice, prima della sua attivazione. Ciò anche esaminando attraverso autonomi procedimenti le caratteristiche degli attuali collegamenti con l'anagrafe tributaria da parte degli enti interessati e le modalità con le quali tali enti intenderebbero integrare la nuova classe di *web services* offerta dall'Agenzia delle entrate nei propri sistemi informativi, ancora in fase di sperimentazione.

Pertanto, con il *provvedimento* 26 novembre 2009 [doc. *web* n. 1679426] considerata l'esigenza di garantire la continuità delle funzioni istituzionali perseguite da Inps, Inpdap, Avcp e Enpals, camere di commercio e Agea con i collegamenti all'anagrafe tributaria in essere, l'Autorità ha consentito a tali soggetti l'utilizzo delle attuali modalità di accesso fino al termine delle verifiche in corso sulla nuova classe di *web service.*

Riscossione a mezzo ruolo

Con *provvedimento* 7 ottobre 2009 [doc. *web* n. 1664231], l'Autorità, nell'ambito degli accertamenti sul sistema informativo della fiscalità, ha individuato una serie di prescrizioni per il trattamento di dati personali effettuato a fini di riscossione a mezzo ruolo. Ciò anche sulla base dei risultati delle ispezioni che hanno riguardato, oltre agli accessi all'anagrafe tributaria da parte degli agenti della riscossione, anche problematiche più generali relative ai trattamenti effettuati a tal fine dall'Agenzia delle entrate, la società Equitalia e le altre società del gruppo.

In tale contesto, il Garante ha tenuto conto della riorganizzazione del servizio di riscossione a mezzo ruolo ancora in corso, volta a dare piena attuazione alla recente e radicale riforma del settore avvenuta ad opera dell'art. 3 del d. l. 30 settembre 2005, n. 203, convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248. In particolare, come è noto, tale riforma ha ricondotto la gestione e la responsabilità della funzione della riscossione in capo all'Amministrazione finanziaria che la esercita mediante la società pubblica Equitalia S.p.A., superando il preesistente impianto concessorio su base provinciale.

Nel *provvedimento* è stato previsto che l'Agenzia delle entrate, Equitalia S.p.A. e le società del gruppo definiscano, entro e non oltre i termini indicati dal Garante, le diverse competenze e responsabilità rispetto al trattamento dei dati. L'Autorità ha prescritto inoltre all'Agenzia delle entrate e alle società del gruppo Equitalia di individuare maggiori garanzie per i contribuenti attraverso informazioni più chiare sull'uso dei dati personali e l'utilizzo di informazioni indispensabili e aggiornate. Ciò consentirà anche un più agevole esercizio dei diritti da parte dei contribuenti che potranno così individuare con più facilità i destinatari cui rivolgere le loro istanze (accesso, rettifica, cancellazione dei dati, *ecc.*). Un'informativa semplice e chiara che indichi, tra l'altro, le rispettive competenze sul trattamento dei dati dovrà comunque essere inserita nell'avviso o nella cartella esattoriale inviata al contribuente.

Un altro aspetto del *provvedimento* ha riguardato l'articolazione delle diverse banche dati utilizzate a fini di riscossione a mezzo ruolo - che Agenzia delle entrate ed Equitalia stanno riorganizzando - al fine di superare le attuali sovrapposizioni che derivano dalla precedente ripartizione sul territorio del servizio della riscossione, evitando rischi per la correttezza dei dati. Equitalia deve, inoltre, assicurare che nel sistema informativo siano contenuti dati il più possibile esatti, aggiornati e pertinenti e che i tempi di conservazione degli stessi siano stabiliti a seconda delle esigenze.

Con riferimento, invece, agli accessi alle anagrafi della popolazione residente, Equitalia S.p.A. deve disciplinare il reperimento delle informazioni anagrafiche da parte delle società del gruppo e deve bloccare i collegamenti effettuati in assenza dei necessari presupposti normativi e delle idonee misure di sicurezza.

Devono, altresì, essere cancellate dai sistemi informativi delle società del gruppo le informazioni eccedenti e non pertinenti le finalità perseguite, con particolare riferimento ai dati anagrafici di soggetti non debitori mai iscritti a ruolo.

Il Garante ha prescritto, inoltre, all'Agenzia delle entrate di elevare le misure di sicurezza per gli accessi effettuati a fine di riscossione all'anagrafe tributaria attraverso l'applicativo Arco (Ausilio riscossione coattiva). Particolari cautele sono, poi, state individuate per quanto concerne l'accesso ai dati trasmessi all'anagrafe tributaria dagli operatori finanziari (ai sensi dell'art. 35, comma 25, del d. l. 4 luglio 2006, n. 223, convertito, con modificazioni, dalla l. 4 agosto 2006, n. 248).

Con riguardo alla fiscalità locale, il Garante ha previsto che l'accesso all'anagrafe tributaria e all'anagrafe dei rapporti finanziari da parte degli enti locali, anche attraverso società esterne, ai fini della riscossione delle proprie entrate ai sensi dell'art. 83, comma 28-s*exies*, del d. l. 25 giugno 2008, n. 112 avvenga solo previa individuazione da parte dell'Agenzia delle entrate di procedure e garanzie idonee a consentire il rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, seguendo i princìpi individuati per la riscossione a mezzo ruolo e nel *provvedimento* 18 settembre 2008.

Con riferimento, invece, all'attività di riscossione spontanea, il Garante ha chiesto a Equitalia di precisare il ruolo svolto dalle società del gruppo nell'ambito del trattamento di dati personali, valutando il grado di autonomia assunto in ordine alle decisioni relative al trattamento delle informazioni e l'ambito di titolarità e responsabilità dell'ente stesso, ed inserendo nelle convenzioni stipulate con gli enti creditori le misure volte a regolare le rispettive attribuzioni e ad assicurare il corretto trattamento delle informazioni. Devono inoltre essere distinti i trattamenti effettuati per la riscossione a mezzo ruolo, prevedendo che i dati siano trattati nel rispetto del principio di finalità attraverso apposite misure organizzative idonee ad assicurare la *"segregazione"* dei dati.

L'Autorità ha prescritto, inoltre, all'Agenzia e ad Equitalia l'adozione di idonee e concrete procedure di *audit* anche periodiche sugli accessi all'anagrafe tributaria effettuati a fini di riscossione, basate sul monitoraggio delle transazioni, nonché su verifiche periodiche, anche a campione, sull'attualità della pendenza soprattutto in relazione ai ruoli

ante riforma. Tali controlli dovranno essere predisposti da Equitalia sulle attività svolte dalle società del gruppo e da Sogei.

Nel rispetto delle competenze loro attribuite dalla legge, il Garante ha impartito prescrizioni analoghe alla Regione Sicilia e alle società che si occupano della riscossione a mezzo ruolo sul territorio regionale.

Scontrino fiscale "parlante"

L'attività istruttoria, di cui si è riferito nella *Relazione 2008* (pp. 75-76), svolta dal Garante con l'Agenzia delle entrate e con i rappresentanti di Federfarma (Federazione nazionale unitaria dei titolari di farmacia italiani) sul trattamento dei dati personali connessi allo "scontrino fiscale parlante" da utilizzare per la deduzione o la detrazione delle spese sanitarie, ha permesso di stabilire che il controllo a fini tributari della natura e della qualità dei farmaci venduti, richiesto dalla legge, può essere effettuato attraverso l'utilizzo del "numero di autorizzazione all'immissione in commercio" (aic) presente sulla confezione di farmaci. Il codice alfanumerico, rilevabile anche mediante lettura ottica, consente, infatti, di identificare in modo univoco ogni singola confezione farmaceutica venduta (dosaggio, somministrazione, presentazione, *ecc.*), al pari della specificazione in chiaro del nome del farmaco.

Nel rispetto della normativa vigente, pertanto, il Garante ha prescritto che, a partire dal 2010, lo scontrino fiscale, rilasciato dalle farmacie per poter dedurre e detrarre la spesa sanitaria nella dichiarazione dei redditi, riporti, in luogo dello specifico nome del farmaco acquistato, l'indicazione del codice alfanumerico posto sulla confezione di ogni medicinale (*Provvedimento* 29 aprile 2009, [doc. *web* n. 1611565]).

Esenzione *ticket*

Il Ministero dell'economia e delle finanze aveva chiesto la collaborazione del Garante per la predisposizione di uno schema di decreto concernente il controllo delle esenzioni sanitarie per reddito.

Con tale atto dovevano essere individuate le modalità con le quali, entro il 15 marzo di ogni anno, l'Agenzia delle entrate, il Ministero del lavoro, della salute e delle politiche sociali e l'Inps devono mettere a disposizione del Servizio sanitario nazionale, tramite l'infrastruttura tecnologica del sistema della tessera sanitaria, le informazioni utili a consentire la verifica della sussistenza del diritto all'esenzione del cittadino in base ai livelli

di reddito previsti dalla legge, con riferimento all'ultimo reddito complessivo del nucleo familiare. Dovevano altresì essere definite le modalità con cui il cittadino è tenuto ad autocertificare la sussistenza del diritto all'esenzione in difformità dalle predette informazioni, prevedendo verifiche da parte delle aziende sanitarie locali competenti circa la conformità delle informazioni rese dal cittadino a quelle disponibili al Servizio sanitario nazionale e le conseguenti sanzioni in caso di mendacio (art. 79, comma 1-*sexies*, lett. *a*) e *b*), d.l. 25 giugno 2008, n. 112, convertito dalla l. n. 133/2008).

Il Garante ha assicurato il proprio contributo al Ministero al fine di individuare nello schema idonee garanzie per la protezione dei dati personali che consentissero l'espressione di un parere favorevole sullo stesso (*Parere* 8 aprile 2009 [doc. *web* n. 1611955]).

In particolare, nello schema è stato previsto che, a seguito dell'elaborazione dei dati mediante l'infrastruttura tecnologica del sistema tessera sanitaria, siano selezionati i soli nuclei familiari dei soggetti assistiti aventi diritto sulla base delle soglie di reddito, della condizione di pensionato e dell'età, associando ad ogni assistito un apposito *"codice di esenzione"* (quest'ultimo reso disponibile unicamente ai medici prescrittori del Ssn e alle aziende sanitarie locali).

Di particolare rilevanza sono risultate poi le misure descritte nella nota tecnica esplicativa inviata dall'amministrazione unitamente allo schema di decreto, quali modalità di archiviazione separata delle informazioni, limiti temporali alla conservazione dei dati in relazione al raggiungimento delle finalità perseguite, nonché particolari cautele che assicurino l'accesso controllato ai dati.

Preoccupazioni sono state espresse dall'Autorità, invece, in relazione alle modalità cartacee di acquisizione delle informazioni da parte dei medici che non dispongono ancora delle necessarie funzionalità informatiche e telematiche, ancorché sia previsto un codice di esenzione per reddito non idoneo a rivelare la specifica condizione di esenzione. A tale riguardo, il Garante ha auspicato l'accelerazione degli adempimenti per superare tale fase transitoria, anche mediante apposite istruzioni fornite dalle aziende sanitarie al personale medico, così da assicurare agli interessati le dovute garanzie, previste a regime per la visualizzazione telematica delle predette informazioni.

Duplicazione codice fiscale e tessera sanitaria

Nell'ambito dell'istruttoria relativa ad un ricorso, è emersa la necessità di verificare il servizio reso dall'Agenzia delle entrate attraverso il suo sito internet, per la richiesta *online* del duplicato del tesserino di codice fiscale o della tessera sanitaria. In particolare, accedendo alla pagina *web* per la richiesta di tale servizio, con l'inserimento di un qualsiasi codice fiscale, il sistema, senza richiedere alcuna identificazione dell'utente, restituiva codice fiscale e dati anagrafici collegati. Anche interrogando il sistema attraverso la maschera di richiesta con l'inserimento di dati anagrafici, veniva restituita una schermata che riportava, oltre a tali dati, anche il codice fiscale, il comune e la provincia di attuale residenza.

Il Garante, pertanto, ha chiesto urgentemente all'Agenzia delle entrate elementi sul punto (*Note* 23 giugno e 1° luglio 2009). L'Agenzia, viste le criticità riscontrate, ha sospeso tempestivamente il servizio, inizialmente predisposto per agevolare l'attività dei contribuenti nei confronti dei propri adempimenti tributari e rendere meno gravose e più efficienti le attività e i servizi erogati dagli uffici territoriali.

Decoder

Il Ministero dello sviluppo economico aveva comunicato al Garante, ai sensi degli artt. 19, comma 2, e 39 del Codice, l'intenzione di acquisire dall'Agenzia delle entrate l'elenco degli abbonati Rai residenti nelle aree interessate dalla transizione alla nuova tecnologia (nuove aree *all digital* 2009), in regola con il pagamento del canone per l'anno in corso, di età pari o superiore a 65 anni (da compiersi entro il 31 dicembre 2009) e un reddito nell'anno 2007 (dichiarazione 2008) pari o inferiore a 10.000 euro.

Il Ministero, infatti, intendeva erogare un contributo per l'acquisto di un *decoder* digitale tramite una riduzione del prezzo, effettuata direttamente nei confronti del destinatario ad opera del rivenditore accreditato, appositamente designato responsabile del trattamento dei dati personali dallo stesso Ministero, con rimborso dell'importo tramite Poste italiane S.p.A. (parimenti designata responsabile del trattamento dei dati). La convenzione stipulata con Poste italiane dal Ministero prevedeva, in particolare, la realizzazione da parte della società di un apposito sito da utilizzare a cura dei rivenditori per le procedure di erogazione del contributo. Il sistema informatico realizzato permetteva quindi ai rivenditori, previa apposita informativa agli interessati in ordine

al trattamento dei dati personali, di verificare e identificare il destinatario del contributo attraverso l'inserimento del codice fiscale dello stesso nella maschera di interrogazione.

Il Garante, nel *provvedimento* 21 aprile 2009 [doc. *web* n. 1611986] ha, quindi, ritenuto che, pur in assenza di un'espressa previsione di legge o di regolamento, l'erogazione dei contributi in favore di famiglie economicamente o socialmente svantaggiate tramite riduzione del prezzo complessivo del *decoder* richiedesse necessariamente la conoscenza dei dati identificativi dei soggetti destinatari. Pertanto, in considerazione della procedura individuata dal Ministero, la comunicazione dei dati da parte dell'Agenzia delle entrate è risultata necessaria, ferma restando l'utilizzabilità delle predette informazioni solo nell'ambito dell'erogazione del contributo.

L'Autorità ha ritenuto a tal fine sufficiente il trattamento dell'elenco dei soli codici fiscali degli abbonati potenzialmente destinatari del contributo, selezionati a cura dell'Agenzia delle entrate sulla base dei criteri predefiniti con apposito atto del Ministero dello sviluppo economico e comunicati dalla stessa Agenzia direttamente a Poste italiane. Il Garante ha evidenziato la necessità che il sistema informatico realizzato da Poste italiane per l'erogazione del contributo assicuri il rispetto delle misure minime di sicurezza previste dall'Allegato B. al Codice, con particolare riferimento alle credenziali di autenticazione del rivenditore e dei suoi collaboratori. L'Autorità ha prescritto inoltre che sia garantita la possibilità di identificare la postazione abilitata ad interrogare il sistema, anche attraverso l'utilizzo di un'apposita modalità di certificazione, e che l'interrogazione dell'elenco dei codici fiscali dei beneficiari restituisca risultati di tipo "booleano" (*ad es.*, vero/falso).

Infine, il Garante ha richiesto che il Ministero determini con precisione i tempi di conservazione, da parte dei rivenditori e di Poste italiane, dei dati relativi a coloro che non hanno richiesto il contributo, con comunicazione di volta in volta al Ministero dell'avvenuta cancellazione delle informazioni.

Il rispetto delle medesime condizioni è stato richiesto dal Garante al Ministero dello sviluppo economico nel *parere* 24 febbraio 2010 [doc. *web* n. 1702875], per l'erogazione del contributo anche nel periodo 2010-2012, nelle aree interessate dalla transizione alla nuova tecnologia, secondo il calendario previsto dal d.m. 10 settembre 2008.

Riutilizzazione commerciale dei dati ipotecari e catastali

Il tema del riutilizzo delle informazioni commerciali e dei dati relativi al comportamento debitorio, com'è noto, è oggetto di specifiche disposizioni del Codice (artt. 118 e 119) in base alle quali è previsto che il Garante promuova la sottoscrizione di un codice di deontologia che deve espressamente individuare, tra l'altro, termini armonizzati di conservazione dei dati personali contenuti, in particolare, in banche di dati, registri ed elenchi tenuti da soggetti pubblici e privati, riferiti al comportamento debitorio dell'interessato nei casi diversi da quelli disciplinati nel codice relativo all'affidabilità e puntualità nei pagamenti, tenendo conto della specificità dei trattamenti nei diversi ambiti.

Nel corso del 2009, l'Agenzia del territorio aveva segnalato al Garante alcune criticità relative al trattamento di dati effettuato da parte degli operatori del settore dell'informazione immobiliare, in particolare, nell'ambito degli accessi al proprio sistema informativo. Tale sistema informativo sarebbe stato, infatti, interessato da significativi disservizi derivanti da comportamenti anomali di alcuni soggetti convenzionati.

Il Garante, dopo aver acquisito alcune specifiche informazioni sul punto, su richiesta dell'Agenzia del territorio, ha quindi deliberato di avviare un tavolo di lavoro tecnico con l'Agenzia stessa per esaminare le problematiche connesse alla riutilizzazione commerciale dei dati ipotecari e catastali (*Nota* 2 febbraio 2010).

3.6. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

Numerose amministrazioni pubbliche si sono rivolte al Garante rappresentando l'intenzione di attivare flussi di dati personali, diversi da quelli sensibili e giudiziari, verso altri soggetti pubblici per lo svolgimento di funzioni istituzionali, in assenza di una norma di legge o di regolamento (artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice).

Tra i casi più rilevanti, si registra quello di una Ausl che intendeva attivare verso un comune flussi di dati relativi all'anagrafe degli assistiti e a quella vaccinale. In proposito, è stato richiamato l'allegato B) dello schema-tipo di regolamento per il trattamento dei dati sensibili e giudiziari di competenza delle regioni, delle province autonome, delle aziende sanitarie, degli enti regionali/provinciali e degli enti vigilati e controllati dalle regioni e dalle province autonome, in conformità al quale ciascuna regione ha adottato

il proprio atto di natura regolamentare nel termine di legge del 28 febbraio 2007 e su cui il Garante ha espresso parere favorevole (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

In particolare, è stato evidenziato che i dati contenuti nell'archivio vaccinale dell'azienda sanitaria possono essere comunicati al comune per l'aggiornamento dell'anagrafe vaccinale comunale (*cfr.* anche Piano nazionale vaccini del Ministero della salute del 2005-2007). Viceversa, i comuni trasmettono periodicamente all'azienda sanitaria gli elenchi nominativi relativi al movimento anagrafico della popolazione relativi ai nuovi nati, deceduti, immigrati e trasferiti per consentire all'azienda stessa di aggiornare la propria anagrafe assistiti (l. 23 dicembre 1978, n. 833). Si è concluso, pertanto, che il flusso di dati tra tali amministrazioni può essere attivato solo in conformità al quadro normativo di settore (*Nota* 23 marzo 2009).

Un comune aveva informato l'Autorità di voler trasmettere ad una società dati anagrafici e tributari necessari per la realizzazione e manutenzione dell'archivio dei soggetti passivi della Tia (tariffa igiene ambientale). In proposito è stato evidenziato che il comune, nell'affidare alla predetta società l'applicazione, la gestione e la riscossione della Tia ai sensi dell'art. 10 del d.P.R. 14 giugno 1990, n. 158, con i conseguenti flussi di dati personali, deve precisare il ruolo svolto dalla stessa nell'ambito del trattamento di dati personali, valutando il grado di autonomia assunto in ordine alle decisioni relative al trattamento delle informazioni e l'ambito di titolarità e responsabilità dell'ente stesso (artt. 4, comma 1, lett. *f*), e 28 del Codice). La predetta società affidataria può essere considerata alternativamente come titolare autonomo o responsabile del trattamento ed in tale ultimo caso, il comune, quale titolare, deve specificare analiticamente e per iscritto i compiti affidati al responsabile, fornendo specifiche istruzioni ed è tenuto a vigilare sul puntuale rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, anche tramite verifiche periodiche (art. 29, commi 4 e 5) (*Nota* 2 settembre 2009).

Un altro comune aveva manifestato il proposito di fornire l'elenco nominativo dei soggetti deceduti in determinati anni, nonché lo stato di famiglia storico aggiornato alla data del decesso dei predetti soggetti, ad un consorzio di bonifica, che ne aveva fatto richiesta

per la revisione del catasto consortile. È stato fatto presente che il rilascio di tali elenchi può essere effettuato in conformità alla specifica disciplina di settore, solamente verso le pubbliche amministrazioni *"che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità"* (art. 34, comma 1, del d.P.R. n. 223/1989 *cit.*) (*Nota* 19 gennaio 2010).

Una società aveva chiesto di poter attivare uno scambio di dati degli utenti che usufruiscono dei servizi di somministrazione di acqua con quelli detenuti da un'altra società, che svolge attività di gestione del servizio di tariffa di igiene ambientale.

Al riguardo è stato rappresentato che nel provvedimento del direttore dell'Agenzia delle entrate adottato il 3 dicembre 2007 (protocollo n. 187461/07, in *G.U.* 17 dicembre 2007, n. 292) - sul quale il Garante ha espresso parere favorevole - in merito alle modalità di partecipazione dei comuni all'accertamento fiscale ai sensi dell'art. 1, comma 2, del d.l. 30 settembre 2005, n. 203, convertito, con modificazioni, dalla legge 2 dicembre 2005, n. 248) è previsto che, entro tre mesi dalla data della sua pubblicazione, l'Agenzia delle entrate renda disponibili ai comuni che ne facciano richiesta i flussi informativi relativi ai contratti di somministrazione di energia elettrica, gas e acqua disponibili in anagrafe tributaria. Pertanto, laddove la trasmissione di dati personali venga effettuata fra soggetti privati non è possibile avvalersi della comunicazione all'Autorità ai sensi delle richiamate disposizioni del Codice; ciò, in quanto un distinto e più stringente quadro normativo disciplina il trattamento dei dati personali da parte dei soggetti privati, anche per quanto riguarda la comunicazione fra gli stessi (artt. 23 *ss.* del Codice) (*Nota* 3 giugno 2009).

Analogo quesito è stato posto dall'Autorità per l'energia elettrica e il gas, sulla convenzione che un gestore dei servizi di fornitura di gas intendeva stipulare con un comune per trasmettergli i dati delle sue utenze da utilizzare per iniziative di contrasto dell'evasione della tassa di igiene ambientale. Al riguardo è stato evidenziato che, sulla base del medesimo quadro normativo, i comuni possono legittimamente ricevere, facendo richiesta all'Agenzia delle entrate, le informazioni necessarie per avviare le iniziative di competenza in materia di contrasto all'evasione (*Nota* 22 febbraio 2010).

In numerosi casi l'Ufficio si è mosso su impulso di cittadini che hanno lamentato,

tramite reclami o segnalazioni, trattamenti non conformi alle disposizioni del Codice in diversi ambiti.

Su segnalazione di un cittadino, l'Ufficio ha chiesto ad un'azienda dipendente da un comune per quali motivi, al fine di erogare taluni buoni sociali, si rendesse necessario trattare dati idonei a rivelare lo stato di salute mediante la documentazione relativa alla certificazione di invalidità ed alla scala *Adl* (*Activities of daily living*, strumento di misura dell'indipendenza funzionale nelle attività di base della vita quotidiana ideato per valutare la prognosi e l'efficacia del trattamento nei soggetti anziani e nei malati cronici) per esteso, invece del solo dato relativo alla percentuale di invalidità e del solo punteggio complessivo finale della predetta scala. All'esito di una complessa istruttoria, l'azienda ha stabilito di richiedere, in occasione della futura erogazione di buoni sociali, la certificazione medica attestante la sola valutazione complessiva relativa alla scala Adl e il verbale di invalidità senza diagnosi, con l'evidenza del solo dato relativo alla percentuale di invalidità (*Nota* 24 giugno 2009).

Era stata altresì lamentata la prassi invalsa presso un comune di riportare sui singoli buoni pasto, che i minori devono poi consegnare al personale scolastico, oltre al nominativo del beneficiario, anche l'indicazione della fascia di reddito del nucleo familiare, nonché la cifra pagata attraverso bollettino postale per usufruire del servizio in questione. A seguito dell'intervento dell'Ufficio, il comune ha stabilito che i nuovi blocchetti non contenessero né il numero della fascia di reddito, né il costo del blocchetto. Sulla base delle predette assicurazioni, non sono state intraprese iniziative per l'adozione di specifici *provvedimenti* da parte del Garante (*v.* artt. 11, comma 1, lett. *d*), e 13, comma 4, del *Regolamento* del Garante n. 1/2007) (*Nota* 15 luglio 2009).

In un altro caso, era stato chiesto di verificare la condotta di un comune che, nel procedere alla trasmissione di comunicazioni tramite servizio postale, riportava sulle buste, oltre al nominativo ed all'indirizzo dell'interessato, anche il codice fiscale ed i dati anagrafici dei destinatari. Al riguardo poiché il sindaco aveva dichiarato che l'inconveniente segnalato era il risultato di un mero refuso relativo ai dati meccanografici, non sono stati ravvisati gli estremi per promuovere l'adozione di un provvedimento da parte

dell'Autorità, fermo restando la competenza dell'autorità giudiziaria ordinaria per il risarcimento di eventuali danni (art. 15 del Codice) (*Nota* 10 novembre 2009).

In relazione ad una notificazione di sanzioni amministrative in busta aperta, effettuata da parte di un comune in mani diverse da quelle del destinatario (art. 174 del Codice), il dirigente responsabile aveva dichiarato che, per l'irregolare procedura di notifica, si sarebbe annullato il provvedimento in questione, nonché verificati i presupposti per una sanzione disciplinare nei confronti degli agenti notificatori. Sulla base di tali assicurazioni non si è proceduto all'adozione di specifici provvedimenti da parte dell'Autorità (*v.* artt. 11, comma 1, lett. *d*), e 13, comma 4, del *Regolamento* del Garante n. 1/2007) (*Nota* 2 novembre 2009).

Sempre in materia di notificazioni, un segnalante aveva lamentato la consegna in mani proprie, ma in busta aperta, per il tramite del messo comunale, di un avviso di accertamento e riscossione della tassa sullo smaltimento dei rifiuti.

A tal proposito è stato evidenziato che la notificazione deve essere effettuata consegnando l'atto in busta sigillata limitatamente alle ipotesi in cui non possa avvenire nelle mani proprie del destinatario (art. 174 del Codice). Inoltre, il trattamento dei dati personali da parte degli incaricati del trattamento (art. 30 del Codice), quali i messi comunali tenuti al segreto d'ufficio, è legittimo (art. 15 del d.P.R. 20 gennaio 1957, n. 3) (*Nota* 10 novembre 2009).

Un cittadino invalido aveva lamentato l'obbligo stabilito da un Comune di inserire determinati tipi di rifiuti (pannolini, pannoloni e rifiuti medicali) in appositi sacchetti di colore giallo, da porre al di fuori della porta o del cancello della propria abitazione, ai fini della raccolta differenziata.

Pur richiamandosi alle garanzie individuate dal Garante con il *provvedimento* del 14 luglio 2005 sulla raccolta differenziata dei rifiuti ([doc. *web* n. 1149822], *Relazione 2005*, p. 39), l'Ufficio non ha ravvisato gli estremi di una violazione del Codice, in quanto il servizio prestato alle utenze è risultato essere svolto a seguito della presentazione di apposita domanda, quindi in forma volontaria. Il Comune si è tuttavia impegnato a valutare altre modalità di conferimento di tali rifiuti (*Nota* 2 novembre 2009).

Era stato posto un quesito in ordine alla mancata indicazione delle generalità dell'agente accertatore nei verbali di contravvenzioni per violazioni del Codice della strada, e al riguardo, richiamando il *provvedimento* adottato dal Garante il 6 febbraio 2001 [doc. *web* n. 41067], è stato ribadito che l'omissione delle generalità dell'organo accertatore non può ritenersi conseguenza dell'applicazione del Codice (*Nota* 5 novembre 2009).

Ad un comune che aveva chiesto chiarimenti in ordine alle corrette modalità per iscriversi ad un *social network*, è stato rappresentato che, in linea generale, non sussistono ostacoli di fondo; tuttavia, iniziative del genere devono avvenire nel rispetto del Codice, nonché di presupposti, limiti e modalità previsti dalla disciplina di settore riguardante singoli atti e documenti.

Più specificatamente, è stata rappresentata la necessità di rispettare le indicazioni fornite con le linee-guida contenute nel *"Rapporto e linee-guida in materia di privacy nei servizi di social network - Memorandum di Roma"* [doc. *web* n. 1567124], con particolare riferimento all'obbligo di assicurare l'esattezza, l'aggiornamento, la pertinenza e non eccedenza dei dati personali, garantendo il rispetto del diritto all'oblìo degli interessati una volta perseguite le finalità poste alla base del trattamento (art. 11, comma 1, lett. *c*), *d*) ed *e*), del Codice). L'ente, infatti, dopo aver valutato se includere i documenti diffusi in eventuali sezioni del sito che li rendano direttamente individuabili in rete, a partire anche da motori di ricerca esterni al sito stesso, deve individuare - opportunamente, con regolamento - periodi di tempo congrui rispetto alle finalità perseguite.

Decorsi tali periodi, determinati documenti o sezioni del sito dovrebbero rimanere in rete, ma essere consultabili solo a partire dal sito stesso (*Nota* 13 gennaio 2010).

I contrassegni per veicoli adibiti al trasporto di persone con disabilità

L'utilizzo dei contrassegni rilasciati per la circolazione e la sosta di veicoli a servizio di persone invalide, ovvero per il transito e la sosta in zone a traffico limitato, è stato oggetto di diversi interventi relativi al trattamento dei dati.

Sul piano normativo è stata esaminata, senza formulare alcun rilievo, una specifica iniziativa del Ministero del lavoro, della salute e delle politiche sociali-Direzione generale per l'inclusione e i diritti sociali e la responsabilità sociale delle imprese volta a modificare l'art. 74 del Codice nella parte che vieta l'apposizione di simboli, al fine di inserire

l'emblema di una sedia a rotelle e rendere così immediatamente riconoscibile la speciale natura del contrassegno rilasciato alla persona disabile.

Il predetto Dicastero ha infatti rappresentato che l'attuale formulazione della norma contrasta con la raccomandazione del Consiglio dell'Unione europea n. 96/376/CE del 4 giugno 1998 sull'adozione di un modello comunitario unico di contrassegno di parcheggio, volto a consentire a tutti i cittadini con disabilità di fruire, nell'area dell'Unione, dei medesimi benefici in termini di circolazione e sosta dei veicoli (*Nota* 15 gennaio 2009).

Un non vedente aveva lamentato che il suo comune di residenza, al fine di consentire l'accesso alle zone a traffico limitato (Ztl) dei soggetti disabili titolari di contrassegno speciale di circolazione, richiedeva di volta in volta la preventiva comunicazione del nominativo dell'accompagnatore al *call center* comunale. Poiché il comune, interpellato sul punto, ha dichiarato che tale comunicazione è prevista dal regolamento comunale relativo alle modalità di rilascio ed utilizzo del contrassegno per la circolazione e la sosta per le persone con disabilità, al fine di scoraggiare l'utilizzo improprio del contrassegno disabili, nel caso di prelievo e/o trasporto del titolare dell'autorizzazione all'interno della zona a traffico limitato, non è stata ravvisata alcuna violazione del Codice da parte del comune medesimo (*v.* artt. 11, comma 1, punto 2, e 13, comma 4, del *Regolamento* del Garante n. 1/2007) (*Nota* 26 giugno 2009).

Un cittadino aveva lamentato l'apposizione della foto della persona fisica interessata, sul retro dei contrassegni rilasciati da un comune per la circolazione e la sosta di veicoli a servizio di persone invalide. Al riguardo, è stato osservato che la disciplina di riferimento dei contrassegni invalidi è costituita, in particolare, dall'art. 188 del nuovo codice della strada (d.lgs. 30 aprile 1992, n. 285), dall'art. 381 del relativo regolamento di attuazione (d.P.R. 16 dicembre 1992, n. 495) e, da ultimo, dall'art. 74 del Codice, da considerarsi, quale norma specifica e posteriore, prevalente sulla citata disposizione legislativa ed, in ogni caso, sul predetto regolamento di attuazione. Pertanto i contrassegni in questione devono contenere i soli dati indispensabili ad individuare l'autorizzazione rilasciata, mentre le generalità e l'indirizzo della persona fisica interessata devono essere riportati con

modalità tali da non permettere la loro diretta visibilità, se non in caso di richiesta di esibizione o necessità di accertamento (art. 74, comma 2, del Codice).

I contrassegni non devono riportare neanche dati personali diversi da quelli previsti quali, ad esempio, la fotografia dell'interessato, la cui apposizione è in contrasto con i princìpi di pertinenza, non eccedenza e indispensabilità dei dati (artt. 11, comma 1, lett. *a*), e 22, comma 3, del Codice).

In tale quadro, è stata vietata al comune l'apposizione della foto dell'interessato sul retro del contrassegno individuando specifici termini per adeguarsi. Pur ritenendo condivisibile l'esigenza di contrastare eventuali abusi, il Garante ha ritenuto a tal fine sufficiente l'indicazione del numero di autorizzazione da cui si può agevolmente risalire al titolare del contrassegno, nonché verificare, se del caso, tramite un documento, l'identità del disabile presente nell'autoveicolo.

3.7. L'ATTIVITÀ GIUDIZIARIA

Pubblicità dei dati nei procedimenti di espropriazione forzata

Nel 2009 si è registrata una diminuzione delle 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 legge 1° maggio 2005, n. 80), che prevede la pubblicazione in appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare.

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, la pubblicazione contestata era stata effettuata in un periodo antecedente al citato *provvedimento* e i dati relativi al segnalante sono stati successivamente oscurati (*Nota* 22 ottobre 2009).

In un altro caso (*Nota* 27 novembre 2009), è stata lamentata una distribuzione di volantini che recavano la pubblicità della vendita all'asta di un immobile nell'ambito del quartiere dove l'immobile medesimo era situato.

Al riguardo, rilevato che il volantino allegato alla segnalazione si limitava a fornire informazioni relative alla vendita giudiziaria senza indicare i nomi degli interessati, si è osservato che ai fini della disciplina in materia di protezione dei dati personali assume rilievo l'eventuale pubblicazione del nominativo del debitore nell'avviso di vendita, mentre esulano dalla competenza dell'Autorità gli aspetti che riguardano la gestione delle forme di pubblicità di tali avvisi.

Pubblicazione di sentenze

Sono pervenute segnalazioni relative alla pubblicazione sui siti istituzionali della Corte di Cassazione e del Consiglio di Stato di sentenze in cui erano riportati i dati identificativi dei segnalanti nonché informazioni relative al loro stato di salute o a rapporti di famiglia.

Al riguardo l'Autorità ha innanzitutto chiarito che l'art. 52 del Codice disciplina esclusivamente l'eventuale pubblicazione di sentenze su riviste giuridiche e siti internet, mentre la pubblicazione mediante deposito dei provvedimenti presso la cancelleria dell'ufficio giudiziario resta disciplinata dalle pertinenti disposizioni dei codici di procedura civile e penale.

L'Autorità ha poi precisato che il comma 5 dell'art. 52 prescrive che chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado deve omettere in ogni caso le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità delle parti nei procedimenti in materia di rapporti di famiglia o di stato delle persone.

È stato infine ribadito che l'art. 22, comma 8, del Codice, in materia di trattamento dei dati sensibili e giudiziari da parte dei soggetti pubblici, vieta la diffusione di dati idonei a rivelare lo stato di salute.

L'Autorità ha pertanto invitato (*Nota* 15 ottobre 2009) i responsabili dei siti istituzionali interessati a oscurare i dati contestati, ottenendo piena collaborazione.

In risposta ad una segnalazione, l'Autorità ha anche avuto modo di precisare che

le pronunce disciplinari emesse dal Consiglio superiore della magistratura hanno natura giurisdizionale, per cui ad esse si applica il regime di pubblicità proprio delle sentenze emesse dall'Autorità giudiziaria. Come previsto dall'art. 51 del Codice, tali pronunce sono quindi conoscibili anche attraverso la rete internet, con le cautele prescritte dal Codice medesimo (art. 52), in caso di loro riproduzione, in ogni forma, per finalità di informazione giuridica (*Nota* 1° luglio 2009).

3.7.1. Trattamenti di dati negli uffici giudiziari

Ruoli di udienza

Nel corso del 2009 è stata lamentata l'affissione, fuori delle aule di udienza di uffici giudiziari, dell'elenco delle cause in trattazione con l'indicazione dei nominativi delle parti. In tale occasione (*Nota* 7 settembre 2009) l'Autorità ha ricordato all'autorità giudiziaria che lo stesso Consiglio superiore della magistratura, con delibera del 23 luglio 2003 ha espressamente ritenuto che "*attesa la non pubblicità delle udienze istruttorie, non sia consentito rendere disponibile per il pubblico il ruolo delle cause chiamate davanti al giudice istruttore. Per le controversie da discutere in udienza pubblica, viceversa, può ritenersi sufficiente l'indicazione, sul ruolo affisso sulla porta della sala dell'udienza, del solo numero del registro generale della controversia, con esclusione di ulteriori riferimenti ai nomi delle parti ed all'oggetto della causa.*"

Accertamenti presso il Gudice di pace

Con delibera del 24 settembre 2009, a seguito di segnalazioni ricevute, il Garante ha avviato accertamenti, ai sensi dell'art. 160 del Codice, in ordine ai trattamenti di dati personali effettuati, per ragioni di giustizia (art. 47, comma 2, del Codice), presso l'Ufficio del Giudice di pace di Roma, relativamente al settore civile. Gli accertamenti, che sono in corso, concernono i trattamenti effettuati sia attraverso il nuovo sistema informatico dei Giudici di pace, sia attraverso la gestione dei fascicoli cartacei.

3.7.2. Notificazioni di atti e comunicazioni

Anche nel 2009 sono pervenute numerose segnalazioni circa modalità di notificazione di atti giudiziari, verbali di contravvenzione e avvisi fiscali non conformi alle prescrizioni del Codice.

Il Garante ha richiamato l'attenzione degli uffici interessati (Unep) al rispetto scrupoloso della vigente normativa, in particolare dell'art. 174 del Codice; questo prevede che, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto deve essere consegnata in una busta sigillata senza indicazioni da cui sia possibile desumere il contenuto dell'atto.

Una segnalazione ha in particolare riguardato la notifica di un atto giudiziario eseguita ai sensi dell'art. 140 c.p.c., secondo il quale *"se non è possibile eseguire la consegna (...) l'ufficiale giudiziario deposita la copia nella casa del comune dove la notificazione deve essere eseguita, affigge avviso del deposito in busta chiusa e sigillata alla porta dell'abitazione o dell'ufficio o dell'azienda del destinatario, e gliene dà notizia per raccomandata con avviso di ricevimento"*.

A tale proposito il Garante ha invitato (*Nota* 13 ottobre 2009) l'ufficio a valutare l'opportunità di adottare maggiori cautele nei casi di affissione dell'avviso di deposito (inserendo, ad esempio, la busta dove è riportata la dicitura *"Ufficio unico esecuzioni protesti"* in altra busta priva di tale indicazione) al fine di tutelare più adeguatamente la riservatezza del destinatario dell'avviso.

In un altro caso (*Nota* 22 maggio 2009) è stata richiamata l'attenzione dell'ufficio giudiziario interessato con riferimento alla fattispecie della notificazione di atti ai militari in servizio ai sensi dell'art. 146 c.p.c.. Si è in particolar modo rilevato che la particolare modalità di notificazione (che prevede la consegna della copia dell'atto al pubblico ministero che ne cura l'invio al comandante del Corpo al quale il militare appartiene) si applica, in via residuale, solo qualora non risulti possibile la notificazione nelle forme ordinarie nelle mani del destinatario e non anche allorché, come nel caso di specie, sia stata eseguita la notificazione con le modalità ordinarie (l'atto era stato notificato direttamente anche all'interessato).

In numerose segnalazioni gli istanti, parti offese in un procedimento penale, avevano lamentato che la notifica dell'avviso di fissazione dell'udienza preliminare sarebbe stata effettuata, in ragione del numero dei destinatari, per pubblici annunzi (art. 155 c.p.p.). Nel rilevare che nella specie tale modalità, pur normativamente prevista, avrebbe

comportato l'indiscriminata diffusione di dati sensibili degli interessati, già individuati da notizie di stampa quali pazienti dell'imputato in quanto portatori di particolari patologie, il Garante ha quindi rappresentato (*Nota* 30 aprile 2009) all'autorità giudiziaria l'opportunità di procedere alle notifiche con le forme ordinarie, al fine di salvaguardare la sfera di riservatezza degli interessati. L'autorità giudiziaria ha accolto l'invito del Garante.

Elezione di domicilio

In risposta ad una segnalazione; è stato, altresì, precisato che non viola la disciplina in materia di protezione dei dati personali l'inosservanza del domicilio prescelto - salvi gli effetti processuali e civili che ne possono derivare, non di competenza dell'Autorità - ove l'invio al domicilio diverso da quello indicato non comporti una comunicazione a terzi di dati personali riferiti agli interessati, come nel caso di invio di plichi chiusi non recanti all'esterno alcuna indicazione idonea a rivelare il contenuto dell'atto (*Nota* 13 ottobre 2009).

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

Il trattamento dei dati personali effettuato dagli esercenti le professioni sanitarie per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato è stato oggetto di specifica attenzione da parte dell'Autorità.

La centralità dell'informativa e del consenso per il trattamento dei dati personali nell'ambito del rapporto medico-paziente è stata più volte richiamata.

In particolare, l'Ufficio ha ricordato ad un ambulatorio di microchirurgia che è necessario acquisire uno specifico consenso informato del paziente per perseguire finalità ulteriori rispetto a quelle strettamente connesse alla cura della salute dell'interessato, nonché per effettuare una comunicazione di dati personali a soggetti terzi (*ad es.*, medico di medicina generale) non prevista dalla legge.

Nella stessa occasione é stato, inoltre, chiarito che devono essere comunicati i soli dati indispensabili preferendo, se possibile, la trasmissione di dati non direttamente identificativi dell'interessato (*ad es.*, laboratorio di analisi). A seguito di tali chiarimenti, lo studio medico ha modificato i modelli di informativa e di consenso utilizzati nei rapporti con i pazienti (*Nota* 18 marzo 2009).

Analogamente, l'Ufficio ha ricordato ad uno studio medico pediatrico che la comunicazione a terzi (*ad es.*, l'azienda sanitaria territoriale) dei dati sanitari dei pazienti può essere effettuata esclusivamente se prevista da una norma di legge, o previo specifico consenso informato dell'interessato o dell'esercente la potestà genitoriale nel caso di minori (artt. 76 *ss.* del Codice).

L'Ufficio ha inoltre ricordato che l'Autorità ha adottato un modello semplificato di informativa per il trattamento dei dati personali effettuato da medici di medicina generale e pediatri di libera scelta da utilizzare facoltativamente nei rapporti con i loro assistiti (*Provv.* 19 luglio 2006, in *G.U.* 8 agosto 2006, n. 183 [doc. *web* n. 1318699]) (*Nota* 12 febbraio 2009).

Con riferimento al trattamento dei dati sanitari mediante sistemi di *Rfid* l'Ufficio, nel richiamare un'azienda ospedaliera al rispetto del *provvedimento* generale del 9 marzo 2005 [doc. *web* n. 1109493], ha ricordato che è necessario raccogliere uno specifico ed informato consenso dell'interessato per l'impiego di tali sistemi nell'ambito del monitoraggio del percorso diagnostico-terapeutico del paziente, nonché segnalare l'esistenza di "rilevatori di passaggio", qualora si reputi indispensabile installare tali lettori (*Nota* 25 febbraio 2009).

Merita, altresì, menzione l'intervento riguardante il trattamento dei dati sanitari rilevabili attraverso l'interrogazione di dispositivi cardiaci impiantati sul paziente.

Al riguardo, l'Ufficio ha osservato che, ferma restando la conoscibilità di tali dati da parte del personale medico che assiste l'interessato a fini di cura della sua salute, l'accesso della società produttrice alle informazioni elaborate da tali apparecchiature deve essere limitato a casi di stretta indispensabilità. In particolare, la società può, di regola, accedere ai dati relativi alla funzionalità dell'apparecchio installato senza associare i dati sanitari rilevati con quelli direttamente identificativi del soggetto su cui il dispositivo è stato impiantato (*Nota* 7 aprile 2009).

In merito al trattamento di dati sanitari nell'ambito di pubblicazioni a contenuto scientifico o finalizzate all'educazione, alla prevenzione o all'informazione di carattere sanitario, era stato chiesto se la pubblicazione da parte del medico curante di alcune lettere su internet, nelle quali i pazienti gli riferiscono informazioni relative all'evoluzione di uno stato patologico, possa porsi in contrasto con la disciplina in materia di protezione dei dati personali.

Al riguardo, l'Ufficio ha osservato che tale operazione costituisce una diffusione di dati sanitari espressamente vietata dal Codice e che nelle pubblicazioni scientifico-sanitarie i medici devono riportare i dati clinici o osservazioni relative a singole persone assicurandone la non identificabilità (*cfr. autorizzazione* generale del Garante n. 2/2009, in *G.U.* 18 gennaio 2010, n. 13 [doc. *web* n. 1682956] e codice di deontologia medica) (*Nota* 3 giugno 2009).

Tra i casi di maggior rilievo si evidenzia l'intervento in materia di sistema di

sorveglianza sanitaria in relazione alla pandemia dell'infezione da *virus* A(H1N1).

Al riguardo, l'Ufficio ha fornito alcune indicazioni ad una associazione di *tour operator* italiani in merito alla possibilità che un operatore turistico possa comunicare - dietro specifica richiesta - all'azienda sanitaria locale (Asl), che ha in cura un paziente affetto da tale influenza, l'elenco dei soggetti che hanno partecipato a viaggi o hanno soggiornato insieme al malato.

L'Ufficio, nel precisare che i dati anagrafici dei compagni di viaggio dell'individuo affetto dall'influenza A(H1N1) non possono considerarsi dati sensibili, in quanto non sono di per sé idonei a rivelare lo stato di salute di taluni soggetti, ha osservato che tale trattamento configura una comunicazione di dati personali da parte di un soggetto privato (operatore turistico) verso un soggetto pubblico (Asl). Tale comunicazione, ammissibile per il raggiungimento di finalità istituzionali dell'azienda (nel caso di specie la profilassi e il controllo sulle malattie infettive e diffusive), può essere effettuata senza richiedere il consenso degli interessati (art. 24, comma 1, lett. *a*), del Codice).

Come precisato anche in alcune circolari del Ministero della salute, in funzione del rafforzamento delle attività di sorveglianza e raccolta dati sui casi confermati di influenza A(H1N1), l'indagine epidemiologica è curata dalla azienda sanitaria di competenza che ha il compito di raccogliere i dati anagrafici e i recapiti dei contatti della persona affetta dall'influenza, mentre il Ministero della salute e l'Istituto superiore di sanità, nell'ambito delle rispettive competenze istituzionali, non hanno la possibilità di accedere ai dati anagrafici dei casi e dei relativi contatti (*Nota* 16 settembre 2009).

Le linee-guida in tema di fascicolo sanitario elettronico (Fse) e di *dossier* sanitario

In termini più generali, nel quadro del processo di ammodernamento della sanità pubblica e privata, il Garante ha avvertito l'esigenza di delineare specifiche garanzie e responsabilità in ordine alla condivisione da parte di distinti titolari del trattamento delle informazioni sanitarie che ricostruiscono la storia sanitaria di un individuo.

Dopo un'ampia procedura di consultazione pubblica (*cfr. Relazione 2008*, p. 17 e *deliberazione* n. 8 del 5 marzo 2009, in *G.U.* 26 marzo 2009, n. 71 [doc. *web* n. 1598313]), e tenuto conto delle osservazioni formulate dal gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali, al quale l'Autorità

ha partecipato in qualità di osservatore, tali garanzie sono state individuate nelle *"Linee-guida in tema di fascicolo sanitario elettronico (Fse) e di dossier sanitario"* (*Provv.* 16 luglio 2009, in *G.U.* 3 agosto 2009, n. 178 [doc. *web* n. 1634116]).

La mancanza a livello nazionale di una definizione normativa di fascicolo sanitario elettronico e di *dossier* sanitario ha indotto il Garante a formulare nel citato *provvedimento* una definizione convenzionale di tali strumenti. In tal senso, si intende per Fse/*dossier* l'insieme delle diverse informazioni inerenti lo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (*ad es.*, referti, documentazione su ricoveri) volte a documentarne la storia clinica. Il suddetto insieme di dati sanitari risulta diversamente denominato in funzione dell'ambito di operatività: il *dossier* è costituito dall'insieme dei dati clinici generato da un organismo sanitario in qualità di unico titolare del trattamento (*ad es.*, azienda ospedaliera), mentre il Fse è originato da diversi titolari del trattamento operanti, generalmente, in un medesimo ambito territoriale.

In assenza di una normativa di settore che preveda il perseguimento, da parte di soggetti pubblici, di specifiche finalità amministrative attraverso il trattamento dei dati personali raccolti mediante il Fse, il Garante ha ritenuto che si possa ricorrere a tale strumento solo per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato, ovvero per assicurare un migliore processo di cura attraverso la ricostruzione - di regola su base logica - il più completa possibile, degli eventi di rilievo clinico occorsi allo stesso.

Il perseguimento delle suddette finalità di cura impone il rispetto del princìpio di autodeterminazione dell'interessato (artt. 75 *ss.* del Codice) al quale, pertanto, deve essere riconosciuto il diritto di scegliere, in piena libertà, se far costituire o meno un proprio Fse/*dossier*. In caso negativo, i dati sanitari resteranno disponibili solo per il professionista o organismo sanitario che li ha redatti, senza alcun pregiudizio per l'accesso dell'interessato alle cure mediche richieste.

Il consenso alla costituzione del Fse deve essere autonomo, specifico e basato su un'adeguata informativa per risultare effettivamente libero (artt. 13, 79 e 80 del Codice). Deve essere altresì prevista la possibilità che l'interessato esprima un consenso di carattere generale per la costituzione del Fse e consensi specifici per la consultazione del medesimo

da parte dei singoli titolari del trattamento (*ad es.*, medico di medicina generale).

È stata inoltre prevista la possibilità di revocare il consenso prestato; in tal caso il Fse/*dossier* non deve essere ulteriormente implementato, restando i documenti sanitari disponibili solo all'organismo che li ha redatti e per eventuali conservazioni per obbligo di legge (art. 22, comma 5, del Codice).

Inoltre deve essere concessa all'interessato la possibilità di non far confluire nel Fse/*dossier* alcune specifiche informazioni sanitarie così come, in generale, il paziente può decidere di non informare il medico di alcuni eventi sanitari che lo riguardano.

L'esercizio di tale scelta da parte dell'interessato non deve essere automaticamente conoscibile da parte del medico che accede al Fse/*dossier* (*cd. "oscuramento dell'oscuramento"*).

Secondo le linee-guida, al Fse/*dossier* possono accedere solo i soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, organizzazioni scientifiche e organismi amministrativi anche operanti in ambito sanitario. Analogamente, l'accesso è precluso anche al personale medico nell'esercizio di attività medico-legale (*ad es.*, visite per l'accertamento dell'idoneità lavorativa), in quanto tali professionisti svolgono la loro attività professionale nell'ambito dell'accertamento di idoneità o *status*, e non anche all'interno del processo di cura dell'interessato.

L'accesso ai documenti contenuti nel Fse/*dossier* è sempre consentito ai soggetti che li hanno redatti, nonché agli altri che abbiano in cura l'interessato, sempre che quest'ultimo ne abbia autorizzato l'accesso nei termini sopra indicati e, comunque, solo per il periodo di tempo indispensabile per espletare le operazioni di cura.

Nei casi in cui si intendano inserire nel Fse informazioni particolarmente delicate, quali quelle relative ad atti di violenza sessuale o di pedofilia, allo stato di sieropositività o all'interruzione volontaria della gravidanza, è necessario acquisire uno specifico consenso dell'interessato.

L'Autorità ha inoltre prescritto a tutti i titolari che i trattamenti di dati personali effettuati attraverso il Fse siano comunicati al Garante entro il 31 dicembre 2009 secondo un modello appositamente individuato. Tale scelta risponde all'esigenza di improntare tali progetti a criteri di massima trasparenza nella loro strutturazione e nel loro funzionamento.

Consultazione *online* dei referti medici

Sempre nell'ambito del processo di ammodernamento della sanità pubblica e privata l'Autorità, con l'adozione delle *"Linee-guida in tema di referti online"* (*Provv.* 19 novembre 2009, in *G.U.* 11 dicembre 2009, n. 288 [doc. *web* n. 1679033]), ha fornito alcune indicazioni anche in merito ai servizi gratuiti generalmente riconducibili all'espressione "referti *online*" (servizi consistenti nella possibilità di ricevere via posta elettronica o di consultare telematicamente il referto) per individuare uno specifico quadro di garanzie per i cittadini.

Le predette linee-guida sono state sottoposte preliminarmente ad una consultazione pubblica, per acquisire osservazioni e commenti da parte degli organismi e professionisti sanitari pubblici e privati e delle associazioni di pazienti interessati (*Deliberazione* n. 21 del 25 giugno 2009, in *G.U.* 15 luglio 2009, n. 162 [doc. *web* n. 1630271]).

La mancanza di specifiche disposizioni normative ha indotto l'Autorità a considerare facoltativa tale modalità di consegna dei referti: l'interessato deve, infatti, poter scegliere - in piena libertà - se accedere o meno al servizio di refertazione *online*, senza nessuna conseguenza sulla possibilità di usufruire delle prestazioni mediche richieste. Resta ferma quindi anche la possibilità di continuare a ritirare i referti in formato cartaceo presso la struttura erogatrice della prestazione sanitaria.

Qualora l'utente scelga i suddetti servizi di refertazione *online* deve essergli concesso, in relazione ai singoli esami clinici, di manifestare una volontà contraria.

Il consenso alla comunicazione dei risultati diagnostici al medico curante, o al medico di medicina generale indicato dal paziente, deve essere manifestato di volta in volta; all'interessato deve, infatti, essere concessa la possibilità di scegliere quali referti mettere a disposizione del proprio medico.

Nel caso di utilizzazione del servizio di avviso, tramite *Sms,* della disponibilità alla consultazione dei referti attraverso le modalità sopra descritte, il Garante ha previsto che nel messaggio inviato sia data solo notizia della disponibilità del referto e non anche del dettaglio della tipologia di accertamenti effettuati, del loro esito o delle credenziali di autenticazione assegnate all'interessato per la consultazione del referto.

Al fine di rispettare la regola dell'intermediazione del medico nella comunicazione

all'interessato di informazioni relative al suo stato di salute, l'Autorità ha previsto che la comunicazione del referto sia accompagnata da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato.

Il Garante ha inoltre ricordato ai titolari del trattamento che, nell'offrire tali servizi, devono tenere conto delle disposizioni di settore che prevedono una specifica attività di consulenza da parte del personale medico (*ad es.*, nel caso di indagini cliniche volte a rivelare direttamente o indirettamente l'infezione da Hiv).

La necessità di assicurare una consulenza genetica appropriata nell'effettuazione di test genetici - anche prenatali - ha indotto l'Autorità ad escludere che tali servizi di refertazione possano essere offerti all'interessato che si sottoponga alle suddette indagini cliniche.

La particolare delicatezza dei dati personali trattati mediante i servizi di refertazione *online* ha indotto a prevedere specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza ai sensi dell'art. 31 del Codice, ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 *ss.*). In particolare, nel caso di consultazione *online* dei referti tramite servizi *web* accessibili da internet, devono essere assicurati protocolli di comunicazione sicuri, basati sull'utilizzo di *standard* crittografici per la comunicazione elettronica dei dati (*Ssl - Secure Socket Layer*), con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete, nonché tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel *file* elettronico nel caso di una sua memorizzazione intermedia in sistemi di *caching*, locali o centralizzati, a seguito della sua consultazione *online*. E' stato inoltre previsto che il referto possa essere disponibile per la consultazione *online* solo per un periodo di tempo limitato di quarantacinque giorni.

Qualora il titolare del trattamento intenda inviare copia del referto alla casella di posta elettronica dell'interessato, il referto in formato digitale deve essere spedito in forma di allegato a un messaggio e-mail e non come testo compreso nella *body part* del messaggio; il *file* contenente il referto deve essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinate.

4.1.2. I trattamenti per fini amministrativi

L'Autorità è stata più volte chiamata nel 2009 a fornire indicazioni in merito ai trattamenti di dati sensibili e, in particolare, di quelli idonei a rivelare lo stato di salute, effettuati da parte di strutture sanitarie pubbliche per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale (art. 85, comma 1, lett. *a*), del Codice).

Al riguardo, l'Ufficio ha ricordato che per finalità amministrative correlate a quelle di cura non è necessario acquisire il consenso dell'interessato, bensì 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 delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali, nonché degli enti vigilati dalle regioni/province autonome, su cui il Garante ha espresso parere favorevole (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

Ad oltre tre anni dall'adozione da parte delle regioni dei suddetti regolamenti, l'Ufficio ha partecipato ad un tavolo di lavoro interregionale istituito per revisionare il predetto schema-tipo di regolamento, anche alla luce dei numerosi interventi normativi che hanno modificato le attività amministrative svolte dalle strutture sanitarie pubbliche.

Per quanto riguarda le finalità amministrative correlate alla cura, l'Ufficio ha specificato che la registrazione delle conversazioni effettuate con la centrale operativa del 118, sebbene non specificamente prevista nella scheda del predetto schema-tipo di regolamento relativa all'assistenza sanitaria fornita in emergenza, può essere comunque effettuata qualora il titolare del trattamento la consideri indispensabile al raggiungimento della finalità di rilevante interesse pubblico perseguita. È stato in particolare chiarito che l'elencazione delle modalità del trattamento non costituisce un elemento essenziale e vincolante delle schede che compongono il suddetto schema-tipo. I dati in tal modo registrati possono essere conservati solo per il periodo strettamente necessario allo svolgimento dell'attività di soccorso, ferme restando le eventuali esigenze in ambito giudiziario e le specifiche eventuali previsioni contenute nella disciplina di settore o contrattuale, nonché le salvaguardie sancite in ambito lavorativo (*cfr.* art. 113 del Codice) (*Nota* 26 febbraio 2009).

Con riferimento all'attività posta in essere dai comuni in merito ai trattamenti sanitari obbligatori (Tso) ed all'assistenza sanitaria obbligatoria l'Ufficio, su segnalazione di un ente, è intervenuto ricordando che la scheda del richiamato schema-tipo di regolamento relativa a tali attività amministrative non prevede che siano comunicati alla questura dati anagrafici dei soggetti sottoposti a Tso. Tale comunicazione di dati sensibili non risulta, inoltre, autorizzata da altra disposizione di legge (*Nota* 11 febbraio 2009).

L'Ufficio si è altresì occupato di una segnalazione relativa all'acquisizione di dati sanitari dei pazienti effettuata dal servizio di portineria di un ospedale e finalizzata alla procedura di ricovero. Al riguardo, l'Ufficio ha ricordato che tale attività costituisce un trattamento di dati sulla salute e, pertanto, può essere legittimamente effettuato solo da parte del personale deputato a prestare le attività di cura all'interessato e di quello incaricato a svolgere le attività amministrative strettamente correlate. A seguito dell'intervento dell'Ufficio, l'ospedale ha previsto che non siano più raccolti dal servizio di portineria documenti dai quali possano emergere informazioni sanitarie dei pazienti (*Nota* 17 luglio 2009).

L'Autorità è stata poi chiamata a fornire alcune indicazioni in merito alla procedura di segnalazione delle corrette modalità di dispensazione di una specialità medicinale, adottata da un servizio regionale per l'assistenza farmaceutica. Il servizio, a seguito delle lamentele ricevute da alcuni assistiti che si erano visti rifiutare l'acquisto del farmaco, aveva emanato una circolare in cui si indicavano alle aziende sanitarie del territorio le cautele vigenti per la vendita di tale farmaco. In tale circolare, tuttavia, si indicava anche l'identità dei soggetti che avevano segnalato la vicenda.

Al riguardo, l'Ufficio ha evidenziato che il riferimento ai nominativi dei soggetti coinvolti non era necessario. Il servizio regionale ha assicurato che nelle future comunicazioni istituzionali sarebbe stata prestata maggiore attenzione alla tutela dei dati personali dei soggetti coinvolti e che i direttori dei servizi farmaceutici sarebbero stati invitati a non utilizzare ulteriormente i dati personali comunicati loro erroneamente (*Nota* 22 giugno 2009).

L'Ufficio è inoltre intervenuto sulle modalità di acquisizione di copia dei documenti

sanitari detenuti da una azienda sanitaria, da parte del medico che aveva avuto in cura una donna, la quale aveva poi promosso nei suoi confronti un'azione giudiziaria. Al riguardo, l'Ufficio ha rilevato che il professionista, per predisporre la sua difesa in giudizio, deve avanzare specifica istanza di accesso alla documentazione detenuta dall'azienda sanitaria, secondo le modalità previste dalla legge ed in conformità ai princìpi di finalità e liceità del trattamento contenuti nel Codice (*Nota* 5 giugno 2009).

Merita, altresì, menzione l'intervento relativo alla pubblicazione sul sito internet di una azienda sanitaria di tutte le delibere del direttore generale, tra le quali una contenente informazioni idonee a rivelare lo stato di salute del segnalante in qualità di destinatario dell'atto amministrativo. Essendo stati pubblicati sul predetto sito soltanto gli atti adottati nei precedenti quindici giorni, all'atto della ricezione della segnalazione la delibera indicata non era più visualizzabile, ma era possibile accedere a numerose delibere aziendali che non rispettavano i princìpi di pertinenza e non eccedenza dei dati rispetto alle finalità del trattamento indicati nelle *"Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali"* [doc. *web* n. 1407101].

È stato quindi ricordato all'azienda che il quadro normativo vieta di diffondere i dati idonei a rivelare lo stato di salute degli interessati (art. 22). A seguito dell'intervento dell'Ufficio, l'azienda sanitaria ha rimosso le delibere in oggetto e fornito indicazioni a tutte le macro aree aziendali sulle regole da seguire per la pubblicazione delle suddette delibere (*Nota* 1° dicembre 2009).

Con riferimento alla diffusione di dati sanitari sul *web*, nel gennaio 2007 l'Autorità era già intervenuta vietando la pubblicazione sul sito internet di una regione del Bollettino ufficiale in cui erano presenti diverse graduatorie per la concessione di contributi regionali indicanti, tra l'altro, le generalità e le motivazioni di esclusione dalle stesse di circa quattromilacinquecento soggetti disabili (*Provv.* 18 gennaio 2007 [doc. *web* n. 1382026]). A seguito di una segnalazione, l'Autorità ha appurato che sul predetto sito erano ancora presenti le suddette graduatorie, che erano state rimosse solo da alcune pagine del sito. Il Garante, pertanto, nell'accertare l'illiceità del trattamento, ha vietato

alla regione la diffusione dei dati idonei a rivelare lo stato di salute degli interessati contenuti nei documenti relativi agli elenchi e alle graduatorie dei disabili, conoscibili mediante la consultazione in qualsiasi forma del Bollettino ufficiale regionale ed, in particolare, attraverso il sito istituzionale (*Provv.* 17 settembre 2009 [doc. *web* n. 1658335]).

Nell'ambito degli approfondimenti avviati sui trattamenti di dati personali finalizzati alla fidelizzazione della clientela delle farmacie, sono stati acquisiti, con la collaborazione di Federfarma, taluni elementi di valutazione circa l'ampiezza del fenomeno presso gli operatori farmaceutici. Nel frattempo il d.lgs. 3 ottobre 2009, n. 153, pubblicato in *G.U.* 4 novembre 2009, n. 257, in attuazione dell'art. 11 della legge-delega n. 69/2009, ha definito nuovi compiti e funzioni assistenziali per le farmacie pubbliche e private operanti in convenzione con il Servizio sanitario nazionale. Atteso il mutato quadro normativo, il Garante ha ritenuto più opportuno intervenire all'atto della consultazione sulla predisposizione dei decreti di attuazione delle nuove disposizioni, peraltro, espressamente prevista soltanto per l'adozione dell'atto di natura non regolamentare volto a stabilire *"modalità, regole tecniche e misure di sicurezza"* di taluni dei nuovi servizi che potranno essere garantiti agli assistiti presso le farmacie, quali quelli di prenotazione di visite specialistiche, pagamento del *ticket* e ritiro dei relativi referti. In tale ambito, l'Autorità, nell'esprimere il previsto parere, potrà suggerire idonei accorgimenti a tutela della riservatezza degli interessati, tenendo conto anche degli approfondimenti già svolti sui trattamenti di dati effettuati dalle farmacie per la fornitura alla clientela di prestazioni sanitarie aggiuntive a quelle tradizionali tramite l'utilizzo di carte magnetiche.

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

Anche nel 2009 l'Autorità è più volte intervenuta sulle garanzie da adottare nel trattamento di dati personali effettuato in occasione dell'accertamento dell'infezione da Hiv.

Tra i casi più rilevanti, la richiesta di chiarimenti da parte di un ospedale sul comportamento da tenere nel caso di mancato ritiro dei referti positivi di analisi per l'accertamento dell'infezione da Hiv. Occorre, al riguardo, tenere conto delle disposizioni che prevedono l'obbligo per *"gli operatori sanitari che, nell'esercizio della loro professione, vengano a*

conoscenza di un caso di Aids, ovvero di un caso di Hiv" di *"adottare tutte le misure occorrenti per la tutela della riservatezza"* e di comunicare i risultati degli accertamenti diagnostici, diretti o indiretti, *"esclusivamente alla persona cui tali esami sono riferiti"* (art. 5, commi 1 e 4, l. n. 135/1990).

L'Ufficio ha osservato che, qualora le strutture sanitarie intendano offrire, a chi si sottopone ad indagini cliniche, la possibilità di essere avvisati telefonicamente in merito al mancato ritiro dei referti, indipendentemente dal risultato diagnostico, è necessario fornire agli utenti interessati una specifica informativa (art. 13 del Codice), in cui si evidenzi la volontarietà dell'adesione a tale servizio. L'interessato che scelga di non aderirvi deve comunque poter usufruire della prestazione sanitaria richiesta. In ogni caso, i referti non ritirati devono essere conservati in conformità alla normativa vigente. Per scongiurare il rischio di un'indebita conoscenza dei dati sulla salute del paziente, l'Ufficio ha ricordato che è necessario richiedere all'interessato che abbia aderito a tale servizio di indicare un recapito telefonico (mobile o fisso) al quale ricevere la comunicazione relativa al mancato ritiro dei referti, impartendo nello stesso tempo agli incaricati opportune istruzioni affinché, nel qualificarsi, non facciano alcun riferimento al fatto che telefonano per conto dell'ospedale o all'oggetto della telefonata e chiedano di conferire con il solo interessato, per comunicare la sola presenza del referto in ospedale e non anche il risultato diagnostico (*Nota* 19 marzo 2009).

Un'associazione che tutela i diritti delle persone sieropositive aveva segnalato al Garante che in uno studio dentistico odontoiatrico, all'atto dell'accettazione, veniva distribuito ai pazienti un questionario, la cui compilazione avrebbe costituito una condizione indispensabile per accedere ai servizi dentistici offerti dallo studio. Nel suddetto questionario si chiedeva al paziente di evidenziare il proprio stato di salute ed, in particolare, se si era affetti da *"infezione da Hiv (Aids)"*.

Da alcune ricerche preliminari è emerso che tale questionario era utilizzato anche da altri studi medici. Da ciò, il Garante ha rilevato la necessità di formulare prescrizioni, nei confronti non solo dello studio oggetto della segnalazione, ma anche di tutti gli esercenti le professioni sanitarie (*Provv.* 12 novembre 2009 [doc. *web* n. 1686068]

e *Provv.* generale 12 novembre 2009, in *G.U.* 12 dicembre 2009, n. 289 [doc. *web* n. 1673588]). Nel *provvedimento* generale, l'Autorità ha specificato che coloro che esercitano la professione sanitaria non devono raccogliere informazioni sulla sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, se ciò non è indispensabile per il tipo di intervento o terapia che deve eseguire. Il dato sull'infezione da Hiv può essere raccolto dal medico, infatti, solo qualora sia ritenuto necessario in relazione all'intervento clinico da eseguire sul paziente e, comunque, con il suo consenso. Pertanto, nel primo colloquio con il paziente deve raccogliere le sole informazioni sanitarie necessarie ad assicurare una corretta assistenza medica. L'esigenza di raccogliere informazioni sull'Hiv fin dal momento dell'accettazione non può essere giustificata neanche dalla necessità di attivare specifiche misure di protezione per il contagio, poiché la normativa di settore prevede che tali misure siano adottate, nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività.

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

Nel 2009 l'Autorità è più volte intervenuta sulla violazione delle misure a tutela della dignità delle persone in ambito sanitario, previste dall'art. 83 del Codice.

Nel corso degli ultimi anni, il Garante aveva già richiamato numerosi organismi sanitari al rispetto delle misure volte a garantire la dignità della persona e il massimo livello di tutela dei diritti del malato (*cfr. Provv.* generale 9 novembre 2005 [doc. *web* n. 1191411]).

In un caso, in particolare, l'Ufficio ha ricordato l'esigenza di adottare soluzioni tali da prevenire, durante i colloqui o la raccolta della documentazione di anamnesi, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute, nonché di introdurre cautele volte ad evitare che le prestazioni sanitarie avvengano in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti (*Nota* 6 maggio 2009).

In un altro caso, l'Ufficio ha ricordato che il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per

svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate (artt. 30 e 29 del Codice).

Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al pari del personale medico ed infermieristico, già tenuto al segreto professionale (art. 9 del codice di deontologia medica del 3 ottobre 1998; art. 4 del codice deontologico per gli infermieri del maggio del 1999), gli altri soggetti non tenuti per legge al segreto professionale siano sottoposti a regole di condotta analoghe.

A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali (artt. 30 e 35 del Codice e punto 19.6 del Disciplinare tecnico Allegato B. al Codice), evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi (*Nota* 16 aprile 2009).

Con specifico riferimento ai trattamenti effettuati all'interno degli studi di medicina generale, l'Ufficio ha ricordato che devono essere adottate idonee cautele per evitare che informazioni sulla salute dell'interessato - come quelle contenute nelle prescrizioni mediche - possano essere conosciute da terzi (*ad es.*, i pazienti presenti in sala di attesa o quelli che erroneamente ritirino un referto non proprio) e che il personale designato incaricato del trattamento (art. 30 del Codice) deve essere istruito debitamente in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato. Le prescrizioni mediche, infatti, possono essere consegnate solo all'interessato o ritirate anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa (*Note* 11 marzo 2009 e 5 giugno 2009).

A seguito degli interventi dell'Ufficio, alcune strutture sanitarie hanno modificato le modalità con cui vengono erogate le prestazioni e i servizi sanitari, nonché adottato specifiche soluzioni più rispettose della riservatezza dei pazienti.

In particolare, una struttura sanitaria ha introdotto ulteriori misure organizzative, tra cui la chiamata non nominativa dei pazienti e disposto l'apertura di medicherie

opportunamente separate e distanziate tra loro per evitare situazioni di promiscuità nella raccolta dell'anamnesi (*Nota* 26 maggio 2009).

Anche nel 2009 l'Ufficio si è occupato dei modelli di certificazioni utilizzati dalle strutture sanitarie per la giustificazione dell'assenza dal lavoro dei pazienti.

Al riguardo, l'Ufficio ha ricordato ad un'azienda ospedaliera che nelle certificazioni per fini amministrativi (*ad es.*, per giustificare assenze dal lavoro) non devono essere apposte indicazioni relative alla struttura in cui il paziente si è recato, dalle quali si possa evincere lo stato di salute.

L'azienda ha di conseguenza sostituito la modulistica non conforme con nuovi moduli nei quali non viene fatta menzione del reparto presso cui il paziente ha avuto accesso (*Nota* 11 marzo 2009).

4.1.5. La ricerca scientifica

Ricerca medica, biomedica ed epidemiologica

Un istituto di ricovero e cura a carattere scientifico, aveva richiesto all'Autorità, ai sensi dell'art. 110 del Codice, l'autorizzazione al trattamento dei dati sulla salute di circa ventimila pazienti affetti da patologie neoplastiche mammarie per condurre uno studio epidemiologico retrospettivo volto all'individuazione del miglior trattamento del carcinoma mammario operabile, anche in assenza del consenso delle persone interessate. L'impossibilità di acquisire il consenso dei pazienti da coinvolgere nella ricerca veniva giustificata con la consistenza del campione oggetto di studio, con la provenienza extraregionale di una parte di questo, con il tempo trascorso dall'originaria raccolta dei dati, nonché con la stima dei decessi intervenuti. Dall'esame delle caratteristiche dello studio, il Garante ha rilevato che questo non avrebbe potuto raggiungere i suoi scopi senza l'identificazione, anche temporanea degli interessati, e che il trattamento era limitato ai soli dati personali contenuti nelle cartelle cliniche di pazienti curati in precedenza dallo stesso Istituto e conservate da questi a norma di legge. Lo studio, inoltre aveva una durata limitata, in quanto l'Istituto intendeva realizzare per il futuro una ricerca di carattere prospettico in relazione a nuovi casi di pazienti in terapia per patologia neoplastica mammaria, previa acquisizione del loro consenso al trattamento dei dati.

Alla luce delle dichiarazioni rese, infine, l'Istituto si impegnava a raccogliere le manifestazioni di volontà di quegli assistiti che si sarebbero nuovamente recati presso la struttura per il *follow-up* e a non comunicare in alcun modo o diffondere le informazioni utilizzate per la ricerca.

L'Autorità ha quindi ritenuto, con il *provvedimento* 16 aprile 2009 [doc. *web* n. 1611936], l'iniziativa meritevole di considerazione, autorizzando l'utilizzo a scopo di ricerca dei dati personali dei pazienti interessati, anche in assenza del loro consenso informato, in ragione dello scopo scientifico perseguito, delle specifiche modalità di trattamento previste, nonché della limitata durata temporale dello studio, anche alla luce delle pertinenti disposizioni (art. 11 del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, Allegato A.4. al Codice [doc. *web* n. 1038384]).

In risposta ad un quesito posto da un altro istituto a carattere scientifico sulla possibilità di contattare i familiari dei pazienti affetti da una particolare tipologia di tumore per accertare la loro disponibilità a partecipare ad uno studio clinico, l'Ufficio ha fatto presente di non ravvisare alcun ostacolo per i profili concernenti la protezione dei dati personali. La procedura prospettata prevedeva infatti che fossero gli stessi pazienti ad acquisire il consenso dei loro familiari ad essere contattati direttamente dall'istituto per ricevere l'informativa relativa al trattamento dei dati finalizzato alla conduzione dello studio e a comunicare alla struttura i nominativi e i recapiti telefonici soltanto di coloro che vi avessero acconsentito. In proposito, l'Ufficio ha evidenziato l'esigenza di indicare chiaramente ai pazienti coinvolti le possibili conseguenze in termini di conoscibilità in ambito familiare dei propri dati sulla salute, nonché di fornire loro idonee istruzioni affinché nell'informare i rispettivi familiari fosse posta in particolare evidenza la facoltatività del conferimento dei dati al fine di essere contattati dall'istituto per le attività di ricerca (*Nota* 17 luglio 2009).

5. I DATI GENETICI

A oltre due anni di applicazione dell'*autorizzazione* generale al trattamento dei dati genetici (*Provv.* 22 febbraio 2007 [doc. *web* n. 1389918]) si è reso necessario avviare un processo di revisione delle disposizioni ivi contenute, anche in relazione all'iniziativa della Società di genetica umana (Sigu) che ha sottoposto all'attenzione dell'Autorità alcune proposte di modifica e integrazione, tenendo in considerazione lo sviluppo delle conoscenze scientifiche in materia (*v. Relazione 2008*, p. 96).

Su tali basi il Garante, in data 19 novembre 2009, ha approvato in via preliminare un nuovo schema di autorizzazione, che tiene conto dell'esperienza maturata e delle osservazioni formulate da qualificati esperti della materia, con particolare riferimento all'aggiornamento delle definizioni utilizzate, ai trattamenti effettuati per la tutela della salute di familiari in assenza del consenso dell'interessato, alle ricerche scientifiche che coinvolgono minori o altri soggetti vulnerabili senza comportare per loro alcun beneficio diretto, nonché alla comunicazione ai familiari dell'interessato di dati genetici indispensabili per evitare un grave pregiudizio per la loro salute. L'Autorità ha quindi inviato tale schema preliminare al Ministro della salute al fine di acquisire il parere del Consiglio superiore di sanità, riservandosi di apportarvi eventuali perfezionamenti anche all'esito delle indicazioni e dei suggerimenti che perverranno (*Nota* 26 novembre 2009).

In attesa della definizione della predetta procedura consultiva, l'efficacia della vigente *autorizzazione* generale è stata prorogata al 30 aprile 2010 (*Provv.* 22 dicembre 2009, in *G.U.* 15 gennaio 2010, n. 11 [doc. *web* n. 1683067]) e potrà esserlo ulteriormente, qualora l'*iter* previsto non si perfezioni nel frattempo.

In altra parte del testo (*par.* 4.1.) si riferisce sull'esclusione delle indagini genetiche dalla refertazione *online*.

6. LA RICERCA STATISTICA E STORICA

Programma statistico nazionale

Nel 2009, il Garante ha espresso due pareri ai sensi dell'art. 6-*bis*, comma 2, del d.lgs. n. 322/1989, su alcune integrazioni relative ai prospetti identificativi dei progetti da inserire nell'Aggiornamento 2009-2010 del Programma statistico nazionale (Psn) 2008-2010 (*Parere* 12 marzo [doc. *web* n. 1605530] e *Parere* 24 settembre 2009 [doc. *web* n. 1657731]).

Come rilevato in precedenti pareri analoghi, il Garante ha ribadito che, qualora i prospetti identificativi di trattamenti di dati personali da inserire nel Psn non riportino le indicazioni necessarie per consentire all'Autorità di esprimere il parere, l'informativa agli interessati deve essere resa con altre idonee modalità. In ogni caso, per fornire l'informativa semplificata tramite il Psn, i prospetti identificativi dei progetti che trattano dati personali devono rendere agevolmente identificabili agli interessati tutti gli elementi indicati dall'art. 13 del Codice.

Inoltre, per quanto riguarda i progetti che comportano il trattamento di dati sensibili e giudiziari, salvo che gli stessi siano già puntualmente individuati da norme di legge o di regolamento, la mancanza di sufficienti elementi per l'espressione del parere favorevole comporta che i dati non potranno essere trattati. Solo dopo una nuova acquisizione del parere del Garante sugli idonei prospetti identificativi inclusi nel Psn, i trattamenti potranno avvenire in modo conforme a quanto ivi riportato.

Con riferimento ai sistemi informativi statistici, l'Autorità ha rilevato che alcuni dei progetti esaminati descrivevano considerevoli trattamenti di dati personali identificativi con interconnessione anche tra informazioni idonee a rivelare lo stato di salute raccolte anche da diversi titolari. Al riguardo, per consentire una corretta lettura dei prospetti identificativi, il Garante ha evidenziato che vi devono essere chiaramente indicate le fonti di dati da cui vengono raccolte informazioni personali.

Il Garante è intervenuto inoltre in relazione alla conservazione dei dati personali, rilevando che tale operazione è ammessa nei soli casi in cui la disponibilità degli stessi dovesse risultare in concreto necessaria per specifiche finalità connesse al trattamento statistico,

da indicare nel prospetto identificativo del progetto.

Qualora sia consentita la conservazione, nell'ambito dei sistemi informativi statistici devono essere adottate misure di carattere tecnologico idonee ad assicurare che essa avvenga nel rispetto del principio di necessità nel trattamento dei dati, nonché della disciplina in materia di segreto statistico.

In ogni caso, i dati personali trattati per scopi statistici devono essere conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

L'Autorità ha inoltre osservato che la costituzione di un sistema informativo statistico rappresenta una delle ipotesi in cui, ai sensi del codice deontologico, la conservazione dei dati identificativi è consentita anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati.

Una volta realizzato il sistema informativo statistico, non è, tuttavia, specificamente contemplata un'ulteriore conservazione dei predetti dati, anche in ossequio al predetto principio di necessità. Specifici rilievi sono stati inoltre effettuati in ordine al sistema informativo Emr-00003-Anagrafe regionale degli studenti della Regione Emilia Romagna, sul quale il Garante ha avviato un autonomo procedimento, provvedendo ad acquisire in loco specifiche informazioni.

Censimento agricolo

Il Garante ha espresso il proprio *parere* ([doc. *web* n. 1703119] *cfr. par.* 1.2.3.) sullo schema di regolamento di esecuzione del sesto censimento generale dell'agricoltura che disciplina tra l'altro i criteri per l'affidamento delle diverse fasi della rilevazione censuaria ad enti od organismi pubblici e privati, i soggetti tenuti all'obbligo di risposta, le modalità di diffusione dei dati, la comunicazione dei dati elementari agli organismi a cui è affidata l'esecuzione del censimento.

Come già osservato dal Garante in occasione delle precedenti rilevazioni censuarie in ambito agricolo e demografico (*cfr. Parere* 29 febbraio 2000 [doc. *web* n. 1085758] e *Parere* 14 marzo 2001 [doc. *web* n. 1075571]), al fine di assicurare la piena conformità delle operazioni alla disciplina in materia di protezione dei dati personali, è necessario garantire che l'Istat sovrintenda alla protezione dei dati personali nella fase attuativa del

censimento. In particolare, l'Autorità ha posto l'attenzione sugli organi di censimento e sugli organismi esterni ai quali vengono affidate le fasi di rilevazione attraverso convenzioni e contratti, nonché sui rilevatori e sui coordinatori, i quali devono ricevere specifiche istruzioni in materia di riservatezza e sicurezza del trattamento di dati personali.

È risultato inoltre necessario suggerire alcune modifiche al testo dello schema di regolamento per assicurare che i dati personali rilevati attraverso le operazioni censuarie siano trattati per soli fini statistici anche presso le amministrazioni che, pur non facenti parte del Sistema statistico nazionale ma presso le quali sia stato costituito l'Ufficio di censimento, li abbiano richiesti per soddisfare il proprio fabbisogno informativo statistico legato al territorio.

Inoltre appare opportuno che in sede di applicazione del regolamento, l'Istat e le amministrazioni interessate curino nel dettaglio gli adempimenti (*ad es.*, la nomina degli incaricati; l'adozione delle misure di sicurezza; l'informativa all'interessato) necessari a garantire che le suddette attività siano conformi alle prescrizioni del Codice.

Con riferimento alle misure di sicurezza, l'Autorità ha ritenuto opportuno che ogni raccolta di dati personali realizzata con la compilazione di *form* con tecnologia *web* accessibili dalla rete pubblica internet, venga assistita da protocolli di cifratura (*Ssl - Secure Socket Layer*) basati su certificati qualificati rilasciati da un'autorità di certificazione, che consentano agli utenti di verificare in maniera certa l'identità dell'ente erogatore del servizio.

Sono stati chiesti al Garante chiarimenti in ordine alla possibilità di rendere ostensibili ad un giornalista che intendeva scrivere un libro di carattere socio-statistico sulla realtà locale, senza riportare le generalità egli interessati, dati (anche idonei a rivelare lo stato di salute degli interessati e dei congiunti, nonché rapporti riservati di tipo familiare) risalenti ad oltre settanta anni fa e riguardanti i minori *cd.* "esposti", ospitati sino al dopoguerra presso un istituto per l'assistenza all'infanzia. Sul punto è stato fatto presente che, laddove il trattamento dei dati personali sia effettuato unicamente per "scopi storici" (art. 4, comma 4, lett. *a*), del Codice), devono essere osservate specifiche disposizioni legislative (artt. 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 [doc. *web* n. 1556419]). In particolare, i documenti conservati negli archivi storici degli enti pubblici territoriali sono liberamente consultabili trascorsi settanta anni dopo la loro data se i dati sono idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare (art. 124, comma 1, lett. *b*), d.lgs. n. 42/2004 *cit.*). Occorre altresì tenere presente che, in relazione a informazioni sullo stato di salute delle persone, l'utente si deve astenere dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile (art. 11, comma 2, del codice di deontologia e di buona condotta *cit.*) (*Nota* 20 gennaio 2010).

È stato recentemente formulato un quesito riguardante una richiesta di accesso volta a conoscere i dati personali della propria "balia" da una cittadina, la cui madre naturale aveva dichiarato alla nascita di non voler essere nominata ed alla quale il comune interpellato aveva opposto che, alla luce del regolamento comunale, gli atti relativi all'infanzia abbandonata diventano consultabili dopo settanta anni.

Al riguardo è stato ricordato che i documenti conservati negli archivi storici degli enti locali sono consultabili trascorsi settanta anni dopo la loro data se riguardano rapporti riservati di tipo familiare; anteriormente al decorso dei predetti termini, i documenti restano accessibili ai sensi della disciplina sull'accesso ai documenti amministrativi (art. 122 d.lgs. n. 42/2004 *cit.*).

In tale quadro, solo il comune può entrare nel merito della richiesta e verificare, anche in conformità al proprio regolamento in materia di accesso ai documenti amministrativi, la sussistenza dei necessari presupposti per rendere ostensibili gli atti richiesti (*Nota* 13 marzo 2009).

7. ATTIVITÀ DI POLIZIA

7.1. IL CONTROLLO SUL CED DEL DIPARTIMENTO DI 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 legge 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

Il 10 settembre 2009 il Garante ha espresso, ai sensi dell'art. 54 del Codice, *parere* favorevole [doc. *web* n. 1658464] su uno schema di Protocollo d'intesa da stipularsi tra il Ministero dell'interno e il Ministero della giustizia, relativo alla trasmissione telematica delle notizie di reato e dei loro esiti tra il Ced del Dipartimento di pubblica sicurezza e le procure della Repubblica.

Il progetto "Notizie di Reato 1"

Il Protocollo disciplina la collaborazione tra le due amministrazioni per dare attuazione al progetto denominato "Notizie di Reato1" (NdR1) con il quale si intende migliorare l'efficienza e la rapidità nell'acquisizione delle notizie di reato da parte delle procure e ridurre i tempi di trasmissione, dalle procure alle forze di polizia, delle conclusioni dei procedimenti penali. Ciò anche al fine di consentire un più rapido e puntuale aggiornamento dei dati personali trattati presso il Ced, nel rispetto dei requisiti di esattezza e completezza nel trattamento delle informazioni.

Il parere favorevole tiene conto dei chiarimenti forniti dai Ministeri dell'interno e della giustizia nel corso di alcuni incontri tecnici tenuti presso l'Autorità. Gli approfondimenti svolti hanno riguardato, in particolare, gli aspetti del progetto relativi alla corretta identificazione delle parti che comunicano fra loro (forze di polizia e procure) e dei sistemi informatici (S.d.i. del Ced e Re.ge. delle procure) che alimentano il flusso tra le amministrazioni; l'esclusiva disponibilità e gestione da parte delle procure delle notizie

di reato trasmesse dalle forze di polizia; la più analitica descrizione delle modalità di accesso e i tipi di informazioni "visibili" relative alle notizie di reato "segretate". Adeguate sono risultate le misure di sicurezza a garanzia del flusso di informazioni tra il Ced e le procure.

7.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

Si è riferito nella *Relazione 2008*, p. 103, del *provvedimento* del 10 luglio 2008 con cui il Garante ha prescritto alcune modificazioni e integrazioni da apportare ai trattamenti effettuati dal Ministero dell'interno-Dipartimento della pubblica sicurezza per l'attuazione della Convenzione.

I riscontri forniti dal Dipartimento hanno permesso di accertare che le prescrizioni sono state adempiute.

Un secondo ciclo di accertamenti, che ha avuto luogo nel corso del 2009, ha riguardato l'adozione da parte del Dipartimento delle misure idonee ad assicurare la sicurezza dei dati relativi alle segnalazioni e dei sistemi utilizzati sia dalla Divisione N-SIS, che gestisce il *database* nazionale, sia dalla Divisione SIRENE, che provvede allo scambio con gli omologhi uffici degli altri Stati aderenti alla Convenzione delle informazioni aggiuntive ritenute utili a dare seguito alle segnalazioni.

All'esito delle verifiche, l'Autorità ha prescritto al Ministero dell'interno un rafforzamento delle misure impiegate. Tra l'altro, gli accessi effettuati al sistema dovranno essere tracciabili e basati su procedure certificate, su cui dovrà vigilare un'unità di *auditing* potenziata e responsabile della sicurezza dei dati. I flussi informativi della Divisione SIRENE dovranno essere effettuati mediante posta elettronica certificata e, laddove si utilizzi il fax, mediante l'adozione di particolari tecniche di cifratura e l'uso di gruppi chiusi di numerazione. La sala *server* delle Divisioni N-SIS e SIRENE dovrà essere protetta mediante l'adozione di una procedura speciale di *strong authentication*, ottenuta dalla combinazione di più credenziali di accesso (*badge* nominale e dispositivo basato su una caratteristica biometrica); dovrà inoltre essere garantita la disponibilità e la continuità di esercizio della banca dati adottando piani di prevenzione che impediscano la sospensione dei servizi.

Il Ministero dell'interno dovrà dare riscontro all'Autorità dell'avvenuta adozione delle misure prescritte.

Accesso diretto

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nell'N-SIS, in virtù delle quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del SIS, ossia al Dipartimento della pubblica sicurezza (*cd.* "accesso diretto"). Il numero e il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante non hanno subito sostanziali variazioni rispetto all'anno precedente (*v. Relazione 2008*, p. 103).

Nel 2009 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 GIORNALISTICA E TECNOLOGIE DELLA COMUNICAZIONE

8.1. MINORI

Nel periodo di riferimento il Garante si è anche occupato del bilanciamento tra libertà di informazione e tutela della riservatezza dei minori.

Vittime di abusi

Dopo il caso di violenza sessuale verificatosi a Roma ai danni di una quattordicenne (*Provv.* 16 febbraio 2009 [doc. *web* n. 1590076] in *Relazione 2008*, p. 104), il Garante ha affrontato un altro grave episodio di abusi su una minore. Anche in tale occasione l'Autorità ha precisato che, pur quando la vittima non viene individuata nominativamente, la diffusione di altre dettagliate informazioni che la riguardano può comunque renderla riconoscibile.

Nel caso di specie erano stati diffusi dati relativi ai soggetti ritenuti responsabili della violenza (il nome e il cognome, l'età e l'attività lavorativa del padre, il nome e l'età del fratello e il nome e il cognome e l'attività svolta dal vicino di casa), nonché dati relativi alla stessa vittima delle violenze (il luogo in cui abitava o residenza, la composizione del suo nucleo familiare). Ciò ha determinato la violazione di regole diverse, in particolare dell'art. 114, comma 6, c.p.p., il quale vieta la divulgazione di elementi che anche indirettamente possano portare all'identificazione del minore e dell'art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (Allegato A.1. al Codice [doc. *web* n. 1556386]) il quale - anche attraverso il richiamo alla Carta di Treviso - considera sempre prevalente il diritto del minore alla riservatezza rispetto al diritto di cronaca e preclude al giornalista la facoltà di diffondere dati idonei ad identificare, anche indirettamente, soggetti minori comunque coinvolti in fatti di cronaca (*Comunicato stampa* 27 gennaio 2010; *Provv.* 28 gennaio 2010 [doc. *web* n. 1696265]; *Provv.* 11 febbraio 2010 [doc. *web* n. 1696239]).

Inoltre in relazione alla notizia di gravi maltrattamenti compiuti in un asilo di Pistoia ai danni di alcuni bambini, il Garante ha tempestivamente richiamato gli organi di informazione a non diffondere le scene dei maltrattamenti senza oscurare in modo adeguato il volto dei minori. Infatti, diversi telegiornali e siti internet, pur nel legittimo intento

di denunciare una simile vicenda, avevano omesso di adottare siffatte cautele esponendo i minori a un ulteriore pregiudizio (*Comunicato stampa* 4 dicembre 2009).

Figli di personaggi pubblici

E' stata poi nuovamente affrontata la questione dei limiti entro cui l'informazione possa coinvolgere anche i figli di personaggi noti, in relazione ad una segnalazione concernente la pubblicazione su un settimanale di immagini di due minori ripresi nella piscina di un albergo insieme al padre e alla sua compagna, entrambi noti personaggi pubblici.

L'Autorità ha ritenuto fondata l'opposizione del genitore alla pubblicazione delle predette foto sulla base del fatto che, nel caso concreto, la pubblicazione poteva ledere la personalità dei minori contravvenendo agli scopi di tutela perseguiti dal codice deontologico (art. 7) e dalla Carta di Treviso (*Provv.* 10 settembre 2009).

L'Autorità ha ritenuto altresì meritevoli di considerazione le doglianze espresse dalla moglie dell'ex Presidente della Regione Lazio in relazione alla pubblicazione di alcuni servizi giornalistici che avevano interessato le figlie, riprese anche in momenti di vita quotidiana.

In tale occasione, l'Autorità ha ritenuto che tale trattamento di dati, pur se avvenuto con l'accorgimento dell'oscuramento dei volti delle giovani, riguardava persone comunque identificabili, e conseguentemente non era giustificato sul piano dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (quali certamente potevano ritenersi quelli in cui si è trovato coinvolto il citato uomo politico) e in contrasto con la *ratio* delle disposizioni a tutela dei minori, volta a salvaguardare personalità ancora in formazione dal clamore mediatico su fatti di vita in cui si trovino coinvolte loro malgrado (*Comunicato stampa* 13 novembre 2009 e *Nota* 11 febbraio 2010).

Il Garante ha invece ritenuto infondato il ricorso presentato da un noto personaggio dello spettacolo il quale lamentava la pubblicazione di una foto della figlia minorenne sulla copertina di un settimanale. Il ricorrente, in particolare, sosteneva che tali immagini sarebbero state acquisite con modalità illecite, perché indebitamente estratte da un video amatoriale, il cui utilizzo era stato concesso da lui stesso e dal coniuge, in esclusiva e a titolo gratuito, a una emittente televisiva per la messa in onda quale *spot* promozionale di un

programma televisivo condotto dallo stesso ricorrente.

Il Garante ha ritenuto lecito tale trattamento rilevando che l'immagine della bambina era già stata volontariamente resa nota al pubblico dagli stessi genitori e che lo stesso filmato risultava facilmente rinvenibile sulla rete internet.

L'Autorità ha poi osservato che la fotografia pubblicata ritraeva comunque la bambina sorridente, in un contesto positivo e quindi tale da non compromettere lo sviluppo della sua personalità (*Provv.* 10 dicembre 2009 [doc. *web* n. 1691407]).

8.2. CRONACHE GIUDIZIARIE

Le vittime di violenze

Sul fronte delle cronache giudiziarie l'Autorità ha ritenuto illeciti dal punto di vista della disciplina in materia di protezione dei dati personali alcuni articoli che hanno trattato due episodi di violenza sessuale.

Nel primo caso era stato diffuso il nome di una donna che era stata oggetto di ripetute violenze sessuali da parte del padre, nel corso di venticinque anni.

Il Garante ha ricordato che l'ordinamento assicura alle vittime di atti di violenza sessuale una protezione rafforzata, con il divieto di diffondere senza consenso le loro generalità o l'immagine, attraverso mezzi di comunicazione di massa (art. 734-*bis* c.p.) e ha rilevato che, nel caso di specie, la violazione di tale disposizione era ulteriormente aggravata dalla descrizione particolareggiata delle violenze subite (*Provv.* 8 aprile 2009 [doc. *web* n. 1610028]).

Nel secondo caso i quotidiani che avevano diffuso la notizia avevano pubblicato, ciascuno in vario modo, una pluralità di informazioni relative alla vittima e alla sua sfera familiare idonee a renderla riconoscibile.

In tale circostanza il Garante ha ricordato che il limite dell'essenzialità dell'informazione (art. 137, comma 3, del Codice e art. 6 del codice di deontologia) deve essere interpretato con particolare rigore quando vengono in considerazione dati idonei a identificare vittime di violenza sessuale, attese la particolare delicatezza di tali accadimenti e la necessità di tutelare la riservatezza delle vittime delle violenze (*Provv.* 2 aprile 2009 [doc. *web* n. 1605613]).

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

Nel corso del 2009 sono pervenute molte segnalazioni e reclami riguardanti la pubblicazione di servizi giornalistici con immagini ritraenti personaggi pubblici.

In particolare il Garante è tornato a pronunciarsi sulla ripresa di immagini concernenti persone all'interno di un parco, di proprietà di un uomo politico (*cfr. Relazione 2007*, p. 79, *Provv.* 18 giugno 2009 [doc. *web* n. 1623306]), nonché di immagini diffuse da alcuni settimanali che ritraevano un noto attore con alcuni ospiti all'interno del parco della sua villa sul lago di Como (*Provv.* 22 dicembre 2009 [doc. *web* n. 1686747]).

L'Autorità ha precisato che è illecito riprendere e utilizzare immagini di persone situate all'interno di una privata dimora senza il loro consenso e con l'uso di tecniche invasive.

In entrambi i casi, l'Autorità ha riscontrato che, a prescindere da ogni valutazione in ordine alla notorietà degli interessati e all'interesse pubblico della notizia, le immagini erano state acquisite con modalità contrastanti con quelle garanzie di trasparenza e di correttezza che - alla luce dell'art. 11 del Codice e degli artt. 2 e 3 del codice di deontologia - devono caratterizzare la raccolta di dati personali, anche nell'esercizio dell'attività giornalistica.

Considerazioni diverse sono state formulate in relazione all'acquisizione di immagini ritraenti persone in luoghi esposti alla visibilità di terzi quali, *ad es.*, un pontile (*Comunicato stampa* 11 settembre 2009), un balcone (*Provv.* 22 dicembre 2009 *cit.*), una spiaggia o l'esterno di una barca (*Provv.* 10 settembre 2009), non trattandosi di aree nelle quali, anche secondo un consolidato orientamento giurisprudenziale, può vantarsi uno *jus excludendi alios* o comunque una ragionevole aspettativa di intimità e riservatezza (tra le numerose decisioni, *cfr.* Corte cost. 16 maggio 2008, n. 149; nonché Cass. pen., Sez. V, 21 ottobre 2008, n. 44156; Cass. pen., Sez. VI, 1 ottobre 2008, n. 40577; Cass. pen., Sez. un., 28 marzo 2006, n. 26795 e Cass. pen., Sez. IV, 16 marzo 2000, n. 7063).

Di regola, dunque, quando le immagini ritraggono persone in luoghi pubblici, aperti al pubblico o comunque visibili da terzi, la loro diffusione è lecita.

Tuttavia anche questa può incontrare dei limiti qualora leda i diritti della persona. In questo senso, si è espresso l'Ufficio del Garante in relazione a un reclamo presentato dalla compagna di un noto esponente istituzionale per la pubblicazione di alcune fotografie che avevano ritratto la coppia su una barca, in momenti di *relax* e di affettuosità. L'Ufficio ha ritenuto il servizio giustificabile in termini generali quale espressione del diritto di cronaca, attesa anche la notorietà dei personaggi (*Nota* 16 ottobre 2009).

Sono state però ritenute eccedenti alcune fotografie che avevano indugiato su alcuni gesti e situazioni di intimità della coppia; ciò, in applicazione dei princìpi del codice di deontologia (art. 1, comma 1, art. 8, comma 1 e art. 11, comma 2) relativi al rispetto dei diritti della persona.

L'Ufficio ha esaminato altresì le ulteriori ragioni poste dalla stessa reclamante alla base della sua opposizione alla riproposizione sulla rete *web* di un video/intervista girato insieme al suo precedente compagno, nel contesto della loro relazione sentimentale risalente nel tempo. Senza mettere in discussione la liceità della diffusione delle immagini e delle notizie attinenti a tale passata relazione - essendo infatti riferibili a personaggi pubblici e a fatti resi noti direttamente dagli stessi interessati o attraverso loro comportamenti in pubblico - è stata tuttavia ritenuta meritevole di considerazione l'esigenza della reclamante di vedere rispettata la sua attuale dimensione sociale e affettiva, in quanto espressione del diritto all'identità personale e quello alla protezione dei dati personali tutelati dall'art. 2 del Codice (*Note* 16 ottobre e 24 dicembre 2009).

Nel pronunciarsi su una segnalazione l'Autorità ha poi ricordato che l'immagine di una persona, anche se nota, non può essere sfruttata commercialmente senza il suo consenso.

Nel caso di specie si trattava di una donna di spettacolo, impegnata anche in politica, che aveva casualmente scoperto la sua fotografia su alcuni volantini pubblicitari utilizzati per reclamizzare servizi odontoiatrici.

L'Autorità ha richiamato quanto stabilito dall'art. 10 c.c. in tema di abuso dell'immagine altrui e dagli artt. 96 e 97 della legge 22 aprile 1941, n. 633 (sulla protezione del diritto d'autore) e ha rilevato una violazione dei doveri di trasparenza

(artt. 11 e 13 del Codice) e di acquisizione del consenso dell'interessato (art. 23) (*Provv.* 12 novembre 2009 [doc. *web* n. 1679779], *cfr. par.* 10.5.).

Pur ribadendo che vi sono più ampi margini nella diffusione di notizie riguardanti i personaggi pubblici, l'Autorità ha tuttavia ricordato che il codice di deontologia pone comunque limiti alla diffusione di notizie e dati relativi alla sfera privata che non hanno alcun rilievo sul ruolo o sulla vita pubblica di tali personaggi (art. 6, comma 3).

In applicazione di tale principio il Garante si è altresì pronunciato sulla segnalazione presentata dal magistrato noto per aver emesso a carico della Fininvest una sentenza di condanna ad un ingente risarcimento. Oggetto della lamentela è stata la diffusione televisiva di un filmato, accompagnato da commenti, che lo avevano ritratto in comuni azioni di vita privata. L'Autorità ha ritenuto il filmato eccedente rispetto a una legittima attività giornalistica, in quanto si era soffermato specificatamente su alcuni particolari comportamenti del giudice o su talune scelte relative al suo abbigliamento prive di ogni connessione o rilievo rispetto al suo ruolo pubblico (*Nota* 18 novembre 2009).

E' stata invece ritenuta infondata la segnalazione presentata da un noto personaggio dello spettacolo, in relazione a un articolo nel quale si era fatto riferimento a suoi presunti orientamenti sessuali. Si è ritenuto infatti che i giudizi e i commenti contenuti nell'articolo rientrassero nell'esercizio della libertà di espressione e nel diritto di critica e di satira, come richiamati anche dall'art. 6, comma 3 del codice di deontologia (*Nota* 23 novembre 2009).

8.4. DATI SULLA SALUTE

Il Garante ha adottato un *provvedimento* di divieto del trattamento nei confronti di un quotidiano che, riferendo il caso di una clinica milanese presso la quale sarebbero stati effettuati alcuni interventi chirurgici al seno risultati non necessari, ha riportato il nome e il cognome delle pazienti, unitamente a descrizioni particolareggiate riguardanti le modalità degli interventi e le patologie delle interessate (*Provv.* 2 aprile 2009 [doc. *web* n. 1605603]).

L'Autorità ha motivato il divieto ricordando che l'ordinamento accorda una speciale

protezione alle informazioni idonee a rivelare lo stato di salute e che *"il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico"* (art. 10 codice di deontologia).

8.5. INFORMAZIONI E SERVIZI *ONLINE*

Sono pervenute al Garante numerose segnalazioni allo scopo di ottenere la cancellazione di dati e di immagini personali diffusi e in vario modo reperibili su internet (*ad es.*, su *E-mule, Youtube, forum, blog*) e reputati lesivi della sfera personale dei segnalanti.

Nei casi in cui ricorrevano i presupposti, e il titolare del trattamento del sito internet segnalato risultava residente in Italia, il Garante è intervenuto chiedendo e ottenendo la cancellazione dei dati personali eccedenti.

In numerosi casi, invece, da verifiche effettuate dall'Ufficio, è risultato che il titolare del trattamento del sito internet interessato non risiedeva in Italia: pertanto, 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, è stata fornita 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 comunitario (*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).

Facebook

In misura superiore rispetto all'anno precedente, nel 2009 sono pervenute segnalazioni con le quali si è lamentato il trattamento illecito dei dati personali su *Facebook*.

Al riguardo si è ritenuto in via preliminare che, ove le immagini e le informazioni restino all'interno di un profilo o di un gruppo chiuso, il trattamento rientra tra quelli per fini esclusivamente personali, non destinati ad una comunicazione sistematica o alla

diffusione, indicati all'art. 5, comma 3, del Codice, e perciò esclusi dall'applicazione della disciplina codicistica; qualora, invece, le informazioni siano visibili in rete in modo libero, e rinvenibili anche tramite i comuni motori di ricerca, poiché si tratta di diffusione, è da ritenersi applicabile integralmente il Codice.

In questo quadro l'Autorità, in un'ottica di collaborazione, in un caso ha contattato il titolare del trattamento (*Facebook*), chiedendo e ottenendo la rimozione dell'indirizzo dell'abitazione della protagonista di uno *spot* televisivo, indirizzo che era liberamente rinvenibile all'interno di un gruppo aperto.

Inoltre sono state ritenute fondate due segnalazioni con cui veniva lamentato che alcuni giornali ed emittenti televisive, a corredo della notizia del decesso di due persone, avevano pubblicato fotografie acquisite direttamente da *Facebook,* attribuendole erroneamente, per pura omonimia, ai deceduti. L'Autorità ha riscontrato in siffatte pubblicazioni una violazione delle disposizioni a tutela del diritto alla protezione dei dati personali e dell'identità personale, essendo state raccolte informazioni non adeguatamente verificate e diffusi dati personali errati (*Provvedimenti* 6 maggio 2009 [doc. *web* nn. 1615317 e 1615339]).

In seguito a queste due segnalazioni, il Garante ha inviato una lettera all'Ordine nazionale dei giornalisti e alla Federazione italiana editori giornali richiamando l'attenzione sui rischi dell'uso della rete internet come fonte di informazioni e di dati personali.

Nel quadro delle medesime problematiche è stata esaminata anche la segnalazione di un professore universitario che ha lamentato un trattamento illecito di dati personali in relazione alla diffusione, nel corso di alcune edizioni di un telegiornale, di una sua fotografia associata al nome di uno sconosciuto, proclamatosi su *Facebook* vincitore al concorso Superenalotto.

L'Ufficio, in considerazione del fatto che l'emittente televisiva ha assicurato di non diffondere in futuro la fotografia, non ha ritenuto di intervenire con un provvedimento inibitorio (*Nota* 24 settembre 2009).

Infine, in seguito alla creazione di un gruppo *choc* contro i bambini *down* apparso su *Facebook* in cui appariva anche la foto di un neonato con una scritta ingiuriosa sulla fronte,

il Garante è intervenuto con un *comunicato stampa* (22 febbraio 2010), invitando i mezzi di informazione che avevano ripreso la foto a non rendere in alcun modo riconoscibile il bambino oggetto dello sfregio.

Giornali *online*, archivi storici e motori di ricerca

Anche nel 2009 il Garante ha ricevuto diverse segnalazioni e ricorsi concernenti la libera disponibilità degli archivi storici *online*.

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

L'articolo infatti era riferito a notizie relative a fatti veri e di interesse pubblico, sia con riferimento al tempo della pubblicazione, sia attualmente per ricerche relative alla vicenda in questione.

In altri casi invece 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 può comportare un sacrificio sproporzionato dei suoi diritti.

L'Autorità in alcuni provvedimenti ha indicato pertanto, quale misura a tutela dei diritti dell'interessato, che la pagina *web* contenente i dati personali del ricorrente (qual è il suo nominativo) sia sottratta alla diretta individuabilità all'atto della ricerca sui comuni motori di ricerca, pur restando tale pagina inalterata nel contesto dell'archivio e consultabile telematicamente accedendo all'indirizzo *web* dell'editore (*Provv.* 25 giugno 2009 [doc. *web*. n. 1635966], *Provv.* 8 aprile 2009 [doc. *web* n. 1617673], *Provv.* 19 novembre 2009 [doc. *web* n. 1689109], *Provv.* 22 dicembre 2009 [doc. *web* n. 1695208]).

In altri casi, invece, il Garante ha ritenuto legittimo il trattamento di dati personali effettuato mediante la riproposizione *online* dell'articolo, in quanto riferito a fatti di persistente interesse pubblico, non ravvisando, pertanto, ragioni per sottrarre l'articolo stesso alla disponibilità dei motori di ricerca.

In particolare, il Garante (*Provv.* 22 maggio 2009 [doc. *web* n. 1635938]) ha dichiarato infondato il ricorso di un politico candidato alle elezioni europee, volto ad ottenere il blocco dei dati personali, pubblicati sul sito di un quotidiano *online,* e relativi alla sua passata attività politica a livello locale e nazionale. Il Garante, infatti, ha ricordato che *"rispetto a persone note, i mezzi di informazione beneficiano (...) di margini più ampi nella pubblicazione di dati e notizie, in particolare nella misura in cui la loro conoscenza assuma un rilievo sul loro ruolo e sulla loro vita pubblica"* (art. 6 del codice di deontologia).

Nel 2009 si è constatata una maggiore sensibilità degli utenti del *web*, nel vigilare e segnalare all'Autorità la non conformità di siti internet alla normativa in materia di protezione dei dati personali.

Consenso degli utenti in fase di registrazione

Sono infatti pervenute diverse segnalazioni relative sia alle informazioni rese agli interessati, sia alle modalità di acquisizione del consenso mediante l'utilizzo di *form online.* Spesso, infatti, le informative pubblicate sui siti sono risultate non sufficientemente chiare e in diversi casi si è riscontrato che la modulistica da compilare per il rilascio del consenso al trattamento dei propri dati è stata predisposta con formulazioni generiche tese a ricomprendere più finalità, tra loro diverse e spesso incompatibili.

L'Autorità ha quindi proceduto alla verifica della conformità dei trattamenti effettuati e talvolta, d'ufficio, delle modulistiche pubblicate sul *web.* Le risultanze di tali accertamenti hanno determinato, per l'anno di riferimento, l'emanazione di due *provvedimenti* contenenti divieto di ulteriore trattamento dei dati e prescrizioni dirette ai titolari del trattamento.

In particolare, a seguito di una segnalazione e al successivo accertamento ispettivo svolto dal Nucleo speciale funzione pubblica e *privacy* della Guardia di finanza in ordine al servizio di biglietteria messo a disposizione su un sito *web*, è risultato che veniva effettuata la raccolta, la conservazione e l'elaborazione dei dati personali dei clienti in relazione a diverse finalità e veniva richiesto un unico consenso indicato come obbligatorio ai fini della registrazione. Il medesimo consenso veniva inoltre richiesto anche con riguardo ai trattamenti effettuati per adempiere alle obbligazioni contrattuali.

Al riguardo con *provvedimento* del 5 marzo 2009 [doc. *web* n. 1615731], l'Autorità

ha essenzialmente ribadito che il titolare del trattamento può prescindere dal consenso per i trattamenti effettuati per eseguire contratti di cui è parte l'interessato (art. 24, comma 1, lett. *b*), del Codice); il consenso, invece, deve essere specificamente acquisito relativamente ai trattamenti per finalità di profilazione e *marketing* (art. 23, comma 3 del Codice).

Il Garante, nel suddetto *provvedimento*, in particolare ha prescritto l'adozione di alcune modifiche al modello per la manifestazione del consenso del trattamento dei dati, affinché quest'ultimo possa essere prestato dagli interessati distintamente per ciascuna diversa finalità perseguita.

Inoltre, si segnala che da accertamenti di carattere ispettivo, è risultato che una società fornitrice di energia raccoglieva, conservava e elaborava dati personali dei clienti in relazione a diverse finalità, tra le quali la realizzazione di attività di vendita o di collocamento di prodotti/servizi, l'analisi delle abitudini e scelte di consumo, nonché l'invio di materiale pubblicitario, anche da parte di terzi, richiedendo, però, un unico consenso.

Quindi con *provvedimento* del 16 dicembre 2009 [doc. *web* n. 1688999], accertati l'illiceità e il carattere sistematico del trattamento dei dati personali effettuato dalla società, il Garante ha vietato l'ulteriore trattamento risultato illecito, e stabilito un termine per documentare l'avvenuta modifica del modello di raccolta del consenso.

8.6. RETI DI COMUNICAZIONE

8.6.1. Invio di comunicazioni commerciali non sollecitate (spam)

Anche nel 2009 il Garante ha ricevuto molte richieste d'intervento relativamente ad attività di *spam* realizzata mediante diversi mezzi (e-mail, fax, chiamate telefoniche, *Sms*).

In più occasioni, anche a seguito di accertamenti ispettivi, l'Autorità ha vietato l'invio, mediante posta elettronica, di comunicazioni promozionali a terzi senza il consenso preventivo, specifico e informato degli interessati ai sensi dell'art. 130 del Codice (*Provvedimenti* 19 febbraio 2009 [doc. *web* nn. 1597146, 1597151], *Provv.* 26 febbraio 2009 [doc. *web* n. 1601506], *Provvedimenti* 22 maggio 2009 [doc. *web* nn. 1621346, 1621355]).

In tali 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 (in tal senso già *provv.* 29 maggio 2003, relativo allo *spamming* [doc. *web* n. 29840]).

In caso di trattamento illecito per l'invio tramite posta elettronica di comunicazioni non richieste, l'Autorità, inoltre, ha provveduto a comminare le previste sanzioni amministrative (in particolare disciplinate dagli artt. 161 e 162, comma 2-*bis* del Codice) e in un caso è stata informata la procura della Repubblica competente, in quanto è stata rilevata l'inottemperanza da parte del titolare del trattamento ad un precedente provvedimento di divieto.

In relazione all'invio di fax pubblicitari a destinatari che avevano ricevuto idonea informativa *ex* art. 13 del Codice, ma che non avevano mai prestato il consenso, sono stati emanati diversi provvedimenti, accompagnati dalle conseguenti sanzioni amministrative (in particolare: *Provv.* 19 febbraio 2009 [doc. *web* n. 1597163], *Provv.* 26 febbraio 2009 [doc. *web* n. 1601475], *Provvedimenti* 22 maggio 2009 [doc. *web* nn. 1621364, 1621340, 1621185], *Provv.* 21 ottobre 2009 [doc. *web* n. 1667012]).

In tali occasioni, l'Autorità ha 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 pubblicitario e commerciale del telefax, in considerazione della specifica disciplina prevista all'art. 130 del Codice.

Sempre in materia di *spam* (in particolare via fax), il Garante ha adottato un *provvedimento* inibitorio e prescrittivo anche nei confronti di una società che, presumendo di poter inviare comunicazioni pubblicitarie in ragione dell'acquisto da terzi di un *database*, non è stata in grado di documentare il consenso del segnalante al trattamento dei suoi dati personali per la ricezione di messaggi promozionali (*Provv.* 22 maggio 2009 [doc. *web* n. 1621185]).

Rispetto allo *spam* mediante *Sms*, il Garante ha prospettato la possibile applicazione

non solo delle sanzioni per omessa o inadeguata informativa e omesso consenso, ma anche della sanzione amministrativa di cui all'art. 162, comma 2-*ter*, del Codice e della correlata sanzione penale di cui all'art. 170 del Codice, per inosservanza di un precedente *provvedimento* inibitorio del Garante.

Più in generale, per l'attività di *spamming*, quando l'Autorità non ha ritenuto sussistere i presupposti per l'adozione di un *provvedimento* inibitorio e/o prescrittivo, ha comunque inviato apposite note di diffida dal proseguire in attività difformi dalla disciplina in materia.

Si segnala, inoltre, che il Garante, per la prima volta, ha vietato l'effettuazione di telefonate commerciali mediante sistemi che generano numerazioni casuali.

Spam telefonico mediante generazione casuale del numero

In particolare, è intervenuto contro una azienda vinicola a seguito delle segnalazioni di numerosi cittadini che lamentavano la ricezione di telefonate indesiderate, in alcuni casi preregistrate (*Provv.* 3 dicembre 2009 [doc. *web* n. 1679436]).

Per tali comunicazioni commerciali l'azienda non aveva utilizzato, direttamente o attraverso i propri *call center*, i numeri presi dagli elenchi telefonici, ma si serviva di un sistema che generava i numeri da contattare attraverso sequenze casuali. Le sequenze erano elaborate secondo criteri geografici e i numeri non erano abbinati a dati anagrafici.

L'Autorità ha precisato che anche il numero casualmente composto e chiamato telefonicamente deve considerarsi "dato personale", in quanto riferibile, anche indirettamente, a una persona identificata o identificabile.

Di conseguenza, in base alla normativa sulla *privacy*, per poter trattare questa tipologia di dati a fini commerciali è necessario il previo consenso dell'interessato, soprattutto quando si utilizzano, quali modalità di contatto, chiamate preregistrate.

Accertata l'illiceità del trattamento, il Garante ha vietato all'azienda di usare tali sistemi, prescrivendo, altresì, la cancellazione di tutti i dati personali per i quali tale consenso non risultasse documentato.

Spam dall'estero

Il Garante in molti casi, a seguito di complesse istruttorie, verificato l'invio di fax da società localizzate all'estero (Francia, Regno Unito, Romania, Spagna, Svizzera, San Marino) ha richiesto la collaborazione delle autorità competenti dei rispettivi Paesi

per far cessare detti invii indesiderati.

Al riguardo, un apposito provvedimento inibitorio a carico della società segnalata è stato adottato dall'Autorità di San Marino.

Si evidenzia, comunque, che il fenomeno appena citato è in costante crescita e l'Autorità sta intensificando la collaborazione su tali temi con le Autorità competenti, in particolare all'interno dell'Ue.

L'Ufficio ha partecipato, inoltre, ad eventi internazionali volti a realizzare una rete di collaborazione tra le autorità e, con il supporto dei soggetti privati, ad arginare il dilagare del fenomeno dello *spam*. In particolare, il Garante ha preso parte a diverse iniziative del *Cnsa* (*The EU Contact Network of Spam Authorities*) a Bruxelles.

8.6.2. La ricerca inversa

Nel corso del 2009 e dei primi mesi del 2010 l'Autorità si è occupata anche del tema della ricerca inversa, ossia della possibilità, per i fornitori di servizi di informazione sugli elenchi, di comunicare a chi ne faccia richiesta, *online* o al telefono, i dati personali degli abbonati presenti negli elenchi telefonici, effettuando la ricerca sulla base del numero telefonico o di altro dato degli stessi.

Il Garante era già intervenuto in materia con il *provvedimento* del 15 luglio 2004 [doc. *web* n. 1032381] stabilendo peraltro che il trattamento dei dati personali nell'ambito dei servizi di informazione sugli elenchi dei singoli operatori deve essere portato a conoscenza degli interessati con un'idonea informativa ai sensi dell'art. 13 del Codice (Allegato I, punto 2.2.) e che l'attivazione della funzione di "ricerca inversa" sui dati degli interessati presuppone il consenso specifico degli stessi (Allegato I, punto 4.2.1.), da raccogliere tramite il questionario contenuto nel modulo di informativa e raccolta del consenso (Allegato IV).

Successivamente all'entrata in vigore del regime degli elenchi telefonici introdotto dal detto *provvedimento*, i fornitori di servizi di informazione sugli elenchi hanno richiesto, con numerose istanze, di modificare la detta disciplina. Hanno infatti rappresentato che la funzionalità del servizio ricerca inversa risultava pregiudicata dalla mancanza dei dati

personali dei vecchi abbonati, i quali non avevano avuto - al momento della stipula del contratto con il proprio operatore telefonico - la possibilità di esprimere il proprio consenso alla reperibilità. Il *database* risultava quindi costituito quasi esclusivamente dai dati personali dei nuovi abbonati che avevano rilasciato il consenso mediante il predetto questionario.

Alla luce di ciò l'Autorità, con un *provvedimento* dell'8 aprile 2010 [doc. *web* n. 1713429], successivamente pubblicato in *Gazzetta Ufficiale*, ha adottato una disciplina differente a seconda se si tratti di vecchi o nuovi abbonati.

In un'ottica di semplificazione, è stato disposto che, con esclusivo riferimento ai "vecchi" abbonati i cui dati erano già inseriti in un elenco pubblico alla data del 1° febbraio 2005, possa essere attivata a partire dal 1° gennaio 2011 la funzione di ricerca inversa anche senza il consenso espresso degli abbonati, salvo il rispetto di eventuali volontà contrarie comunicate dagli stessi al proprio operatore.

Con il medesimo *provvedimento* il Garante, altresì, ha disposto che gli operatori telefonici che abbiano clienti i cui dati erano già inseriti in un elenco pubblico alla data del 1° febbraio 2005 rendano nota a tali abbonati l'attivazione della funzione di ricerca inversa nei loro confronti, mediante idonea informativa, da inserire nella bolletta contenente il conto telefonico entro il 31 dicembre 2010 e da pubblicare sui propri siti *web* entro il 31 maggio 2010, fornendone adeguata documentazione all'Ufficio.

8.6.3. Anomalie nel funzionamento del database *unico (Dbu)*

Nel periodo in esame, il Garante si è occupato della problematica sollevata da alcune società che operano nel settore dell'editoria di elenchi telefonici, nonché in quello della fornitura di informazioni sugli elenchi medesimi concernente il corretto funzionamento della base di dati unica prevista dalla delibera Agcom del 6 febbraio 2002, n. 36/02/CONS (*cd.* "Dbu"), in relazione al trattamento dei dati personali degli abbonati ai servizi telefonici.

In particolare, attualmente il regime degli elenchi telefonici prevede che *"è consentita la sola formazione, distribuzione e diffusione degli elenchi, in qualunque forma realizzati,*

basati sulla consultazione e accesso alla base di dati unica, e che è consentita la sola utilizzazione di elenchi aggiornati" (Allegato III, punto 1, *Provv.* 15 luglio 2004 [doc. *web* n. 1032381]).

Come noto, il Dbu consiste *"nell'insieme dei dati contenuti nelle base dati di tutti gli operatori titolari di licenze per servizi di telecomunicazioni ai quali risultino assegnate risorse di numerazione effettivamente utilizzate"* (art. 2, *par.* 1, delibera Agcom, *cit.*). Sono quindi i singoli operatori telefonici, in qualità di titolari del trattamento, che curano l'inserimento dei dati dei propri clienti, nonché l'aggiornamento periodico degli stessi nel Dbu. Ciò, sulla base dei consensi espressi in risposta al questionario contenuto nel modulo di informativa e raccolta del consenso che ciascun operatore ha sottoposto ai propri clienti per consentire loro di decidere se e con quali informazioni essere presenti negli elenchi telefonici (Allegato IV, *Provv.* 15 luglio 2004, *cit.*).

Viceversa, in relazione ai "vecchi" abbonati alla telefonia fissa, i cui nominativi erano già presenti negli elenchi precedentemente pubblicati, il *provvedimento* del 2004 ha previsto una disciplina transitoria per la quale, in assenza di risposta da parte degli stessi nel termine di sessanta giorni dalla ricezione del predetto modulo, sarebbero rimaste valide le manifestazioni di volontà eventualmente espresse in passato (Allegato I, punto 7.1. e Allegato IV, *Provv.* 15 luglio 2004, *cit.*).

Le società che si sono rivolte al Garante hanno evidenziato come, all'esito di alcune verifiche dalle stesse effettuate sul Dbu, sono state riscontrate numerose anomalie in ordine alla numerosità e alla completezza dei dati forniti evidenziando che, nell'arco di un periodo relativamente breve, si sarebbe registrato un significativo decremento nelle utenze presenti nel Dbu: circa cinquecentomila unità, nel periodo tra marzo e ottobre 2008, e altre duecentocinquantamila utenze fra ottobre 2008 e gennaio 2009.

Le segnalanti hanno ritenuto che il fenomeno della riduzione degli abbonati inseriti nel Dbu fosse dovuto alla mancata compilazione del modulo, di cui all'Allegato IV del *provvedimento* da ultimo menzionato, da parte degli abbonati stessi in occasione del cambio di operatore telefonico.

Il Garante ha quindi adottato il *provvedimento* del 1° aprile 2010 [doc. *web*

n. 1711492], successivamente pubblicato in *Gazzetta Ufficiale*, nel quale ha in primo luogo ricordato che, nel caso in cui un soggetto attivi una nuova utenza telefonica, fissa o mobile, con un operatore diverso dal precedente indipendentemente dal fatto che il "vecchio" contratto di fornitura sia mantenuto in vita o meno, instaurandosi comunque un nuovo rapporto di fornitura di servizi telefonici, il nuovo operatore, in qualità di titolare del trattamento, è tenuto a sottoporre al cliente il modulo di informativa e raccolta del consenso, di cui all'Allegato IV del *provvedimento* del 2004.

L'Autorità ha inoltre ricordato che, anche nel caso in cui l'interessato, al momento dell'attivazione di una nuova utenza con un operatore diverso, decida di conservare il suo numero telefonico, chiedendo la *number portability* (*Np*) si verifica una modifica nel rapporto di fornitura del servizio, poiché cambia il titolare del trattamento. Pertanto, anche in tale evenienza gli operatori sono tenuti a sottoporre all'attenzione dei propri clienti il modello di informativa e richiesta di consenso.

Tuttavia, in ragione del fatto che nell'ipotesi di *number portability* il numero telefonico non cambia e che, quindi, restano invariati tutti gli elementi oggetto di pubblicazione negli elenchi, il Garante ha ritenuto che i clienti che cambiano operatore con *Np*, possano essere assimilati ai "vecchi" clienti presi in considerazione dal *provvedimento* del 2004, ossia quei soggetti i cui nominativi erano già presenti negli elenchi pubblicati prima dell'entrata in vigore del nuovo regime degli elenchi telefonici.

Anche i predetti soggetti infatti hanno già espresso in passato al proprio operatore la volontà di inserimento nel Dbu e, conseguentemente, negli elenchi, dei dati personali che li riguardano.

Il Garante ha quindi stabilito che, per tali soggetti, il nuovo operatore telefonico possa mantenere invariate le opzioni scelte in passato, in assenza di risposta al suindicato questionario nel termine di sessanta giorni dalla ricezione dello stesso, restando naturalmente la possibilità per i medesimi soggetti di manifestare in qualunque momento una diversa volontà, rivolgendosi anche successivamente al nuovo operatore.

8.6.4. Banche dati utilizzate per il telemarketing

A seguito di numerose segnalazioni relative ad attività promozionali effettuate mediante l'invio di materiale cartaceo e contatto telefonico, il Garante ha avviato d'ufficio un'articolata attività istruttoria sull'utilizzo di banche dati per finalità di *marketing.*

Infatti, nonostante gli interventi dell'Autorità (nel corso del 2007 con alcuni p*rovvedimenti* indirizzati a diversi titolari del trattamento [doc. *web* nn. 1412626, 1412610, 1412598, 1412557 e 1412586], *cfr. Relazione 2007*, pag. 83; nel 2008 nei confronti di altri tre soggetti che fornivano alle società telefoniche i *database* utilizzati per campagne di *telemarketing* con altrettanti *provvedimenti* inibitori [doc. *web* nn. 1544315, 1544326, 1544338, 1562780 e 1562758], *cfr. Relazione 2008*, pag. 112) è emerso che il fenomeno del *marketing* indesiderato continua ad assumere un rilievo sempre maggiore.

L'istruttoria aveva preso avvio nel 2008 con una serie di accertamenti ispettivi nei confronti di soggetti che operano nel settore della formazione, gestione e cessione di banche dati e elenchi anagrafici nonché delle altre informazioni utili all'effettuazione di campagne promozionali e che dunque, trattano dati personali per finalità di *marketing* sia in qualità di cedenti che di cessionari di tali *database.*

Modifiche della normativa

Nel corso del 2009 l'utilizzo di dati personali contenuti in banche dati per finalità di *marketing* è stato oggetto di numerosi interventi del legislatore.

Dopo i primi accertamenti ispettivi (settembre 2008–febbraio 2009) è entrata in vigore la disciplina derogatoria e transitoria relativa all'utilizzo delle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005, introdotta dalla legge 27 febbraio 2009, n. 14 (mediante l'emendamento all'art. 44 del d.l. 30 dicembre 2008, n. 207 convertito, con modificazioni, nella citata l., in *G.U.* 28 febbraio 2009, n. 28), sul cui ambito di applicazione il Garante si è espresso con un *provvedimento* di carattere generale adottato il 12 marzo 2009 (*G.U.* 20 marzo 2009, n. 66 [doc. *web* n. 1598808]; *cfr. Relazione 2008*, p.114). I successivi accertamenti ispettivi hanno avuto ad oggetto la verifica della conformità alle prescrizioni contenute in tale *provvedimento.*

Successivamente, l'art. 20-*bis* della legge 20 novembre 2009, n. 166 (*G.U.* 24 novembre 2009, n. 215, con la quale è stato convertito, con modificazioni, il d. l. 25 settembre

2009, n. 135) ha modificato nuovamente la disciplina relativa agli elenchi telefonici, già derogata nei termini di cui sopra.

In particolare, la l. n. 166/2009 ha modificato l'art. 130 del Codice, consentendo il trattamento dei dati tramite contatti telefonici, per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, salvo il diritto di opposizione dell'interessato. La nuova disciplina prevede, quindi, l'istituzione di un "registro pubblico delle opposizioni" entro sei mesi dalla data di entrata in vigore della legge medesima e stabilisce che *"fino al suddetto termine, restano in vigore i provvedimenti adottati dal Garante per la protezione dei dati personali (...) in attuazione dell'articolo 129 del medesimo codice"*.

Alla luce di questo e, in prospettiva dell'attuazione della nuova disciplina, la deroga transitoria e temporanea (che in base al disposto della l. 27 febbraio 2009, n. 14, scadeva il 31 dicembre 2009) è stata prorogata *"sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto legge 25 settembre 2009, n. 135"* (art. 20-*bis*, comma 3, legge 20 novembre 2009, n. 166).

Successivamente a tale modifica legislativa, il Garante ha approvato in data 22 dicembre 2009 un nuovo *provvedimento* ([doc. *web* n. 1683085], in *G.U.* 15 gennaio 2010, n. 11) che ha prorogato l'efficacia del citato *provvedimento* del 12 marzo 2009 sino all'istituzione del predetto registro pubblico delle opposizioni.

Tuttavia occorre rilevare che il nuovo quadro normativo, delineato per esigenze di completezza, dispone per il futuro e dunque ha un impatto limitato sugli esiti dei procedimenti amministrativi relativi alle menzionate società oggetto di ispezione.

Nel complesso, sono state ispezionate dieci società, e redatti venticinque verbali, a ciascuno dei quali sono allegati, mediamente, una decina di documenti anche di carattere tecnico, cui si vanno ad aggiungere i documenti integrativi trasmessi dalle società nei giorni successivi.

L'articolato quadro complessivo emerso dalla totalità delle ispezioni ha evidenziato, in linea generale, un diffuso utilizzo di dati raccolti in violazione delle disposizioni del Codice in materia di informativa e consenso degli interessati.

Tali violazioni hanno determinato l'adozione di ulteriori provvedimenti inibitori e prescrittivi, nonché l'applicazione di sanzioni amministrative per le violazioni previste dal Codice.

In taluni casi, si è resa necessaria la trasmissione degli atti alle competenti procure della Repubblica per l'accertamento di fattispecie di natura penale previste dal Codice (per trattamento illecito dei dati, inosservanza dei provvedimenti dell'Autorità, falsità nelle dichiarazioni al Garante e mancata adozione delle misure minime di sicurezza).

Inoltre, poiché le attività ispettive sono state eseguite durante l'intero arco di tempo in cui il legislatore ha apportato le modifiche al sistema sanzionatorio (dal 1° gennaio 2009), si segnala che l'importo e la natura delle sanzioni amministrative hanno necessariamente tenuto conto della data dell'accertamento.

Per la prima volta, infine, relativamente ad alcune sanzioni amministrative è stata applicata l'aggravante prevista dall'art. 164-*bis*, commi 2 (banche dati di particolare rilevanza o dimensioni) e 3, del Codice, in ragione dell'elevato numero di interessati.

8.6.5. Attività di profilazione della clientela

Con un *provvedimento* generale rivolto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico (*Provv.* 25 giugno 2009 [doc. *web* n. 1629107]) l'Autorità ha stabilito i parametri e le misure minime da seguire per il corretto trattamento dei dati personali dei clienti per finalità di profilazione.

Da un'articolata e complessa attività istruttoria, anche di carattere ispettivo, rivolta a diversi operatori del settore allo scopo di individuare le modalità di svolgimento dell'attività di profilazione della clientela, era emerso che il trattamento di dati personali da parte dei gestori telefonici, diretto ad individuare abitudini di consumo, preferenze e spese telefoniche dei clienti, veniva in molti casi effettuato senza acquisirne il preventivo consenso e senza fornire un'idonea informativa.

L'Autorità è intervenuta per ribadire, in primo luogo, che i dati personali non possono essere utilizzati per tali finalità in assenza di un'adeguata informativa e di un espresso consenso dei soggetti interessati.

Il Garante ha altresì chiarito che le stesse regole operano, in generale, anche con riguardo all'attività di profilazione svolta attraverso dati personali aggregati, i quali non possono, per ciò solo, definirsi come dati anonimi, traendo origine da dati personali presenti in forma completa e dettagliata in una pluralità di sistemi originari che restano nella disponibilità del titolare del trattamento per altre esigenze e finalità ed ai quali è possibile risalire. In tali casi il trattamento può presentare rischi specifici per i diritti e le libertà fondamentali degli utenti, da valutarsi in base alla profondità del livello di aggregazione effettuato dal titolare e alle modalità tecniche utilizzate.

L'Autorità ha tuttavia previsto, per l'attività di profilazione effettuata con l'ausilio di dati aggregati dei clienti di cui non era risultato acquisito il consenso, la possibilità per i fornitori di presentare un'istanza di verifica preliminare, con l'indicazione delle finalità e tipologia dei dati da utilizzare, spettando al Garante valutare, caso per caso, se consentire il trattamento senza l'esplicito consenso degli interessati, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice. Ciò in quanto, l'attività di profilazione rappresenta una delle attività prevalenti degli operatori del settore che vi ricorrono per supportare i propri processi decisionali e strategici.

Entro il termine del 30 settembre 2009, stabilito dall'Autorità per formulare le istanze di *prior checking*, sono pervenute all'Ufficio diverse richieste, in particolare dai sette maggiori gestori di telefonia presenti sul mercato. E' stata perciò condotta un'approfondita istruttoria per ogni singolo operatore, per verificare la sussistenza dei parametri e delle condizioni individuate con il *provvedimento* generale e, conseguentemente l'opportunità di autorizzare il trattamento o di prescrivere eventuali misure specifiche, e i tempi per attuare le prescrizioni indicate.

L'esito di tale attività, che ha comportato un'analisi dettagliata dei sistemi informatici aziendali deputati alla profilazione, anche rispetto alle piattaforme gestionali e agli apparati di rete dei diversi gestori telefonici, ha evidenziato la necessità di emanare una serie di prescrizioni, attraverso *provvedimenti* inviati a ciascun gestore.

Queste ultime hanno riguardato il livello di aggregazione e la tipologia dei dati utilizzati, la separazione funzionale dei sistemi dedicati alla profilazione rispetto a quelli

utilizzati per altre finalità aziendali, come quelle di *marketing*, nonché i processi di mascheramento dei dati personali aggregati, utilizzati per profilare la clientela.

L'Autorità ha inoltre prescritto l'adozione di alcune misure nelle procedure di autenticazione e autorizzazione degli addetti all'attività in parola, individuando un periodo massimo di conservazione dei dati utilizzati, e, al contempo, ordinandone la cancellazione, ovvero la trasformazione irreversibile in forma anonima, alla relativa scadenza.

Ulteriori misure sono state impartite per la revisione dell'informativa da rendere agli interessati ai sensi dell'art. 13 del Codice, con riguardo al trattamento svolto attraverso dati aggregati, nonché per la necessaria notificazione del trattamento ai sensi degli artt. 37, comma 1, lett. *d*), e 38 del Codice.

In ragione della complessità delle misure tecniche previste e delle modifiche da apportare ai sistemi coinvolti nella profilazione, attraverso dati personali aggregati, l'Autorità ha previsto, per l'adozione degli adempimenti prescritti, un termine variabile tra i trenta ed i centottanta giorni.

Con riguardo, invece, all'attività svolta attraverso l'uso di dati personali individuali dei clienti, l'Autorità ha ribadito l'esigenza di acquisire il consenso preventivo, libero e specifico dell'interessato.

In questo ambito, con particolare riguardo alla corretta applicazione degli artt. 13 e 23 del Codice, si ricorda il *provvedimento*, emanato dall'Autorità in materia di *"fidelity card"*, del 24 febbraio 2005 [doc. *web* n. 1103045], nel quale veniva evidenziata la necessità che il cliente fosse messo in grado di manifestare un consenso libero e specifico rispetto a ciascun trattamento di dati chiaramente individuato (art. 23, comma 3), ossia un consenso differenziato per le diverse attività di profilazione e di *marketing* svolte nell'ambito dei servizi di comunicazione elettronica accessibili al pubblico.

9. PROPAGANDA ELETTORALE E ASSOCIAZIONI

Trattamento di dati per finalità di propaganda elettorale

Anche nel 2010 il Garante, in vista delle consultazioni elettorali di marzo-aprile, ha in via temporanea (*Provv.* 11 febbraio 2010, in *G.U.* 22 febbraio 2010, n. 43 [doc. *web* n. 1694531]) esonerato dall'obbligo di informativa - di cui all'art. 13 del Codice - partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati che trattano dati personali per esclusiva finalità di selezione di candidati alle elezioni, di comunicazione politica o di propaganda elettorale.

I suddetti soggetti sono stati esonerati dal rendere l'informativa fino al 30 maggio 2010; decorsa tale data, essi possono continuare a trattare temporaneamente (anche mediante mera conservazione) i dati personali lecitamente raccolti secondo le modalità indicate nel *provvedimento* generale del 7 settembre 2005 (*G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613]), le cui prescrizioni sono state a tal fine integralmente richiamate. Ciò sempreché informino gli interessati entro il 31 luglio 2010, nei modi previsti dal Codice.

Dai predetti *provvedimenti* emergono ulteriori princìpi che devono essere osservati dai soggetti che intraprendono iniziative di selezione di candidati alle elezioni, di comunicazione e di propaganda elettorale.

In particolare, senza il preventivo consenso degli interessati, possono essere utilizzati solo i dati contenuti nelle fonti documentali detenute da soggetti pubblici, liberamente accessibili a chiunque in base a una specifica norma *(ad es.*, le liste elettorali e gli altri elenchi e registri in materia di elettorato attivo e passivo).

I titolari di cariche elettive possono utilizzare le informazioni raccolte nel quadro delle relazioni interpersonali con cittadini ed elettori senza il preventivo consenso degli interessati; tuttavia, non sono legittimati ad ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per attività di propaganda elettorale, così come non sono utilizzabili i dati raccolti nell'esercizio di attività professionali e di impresa.

Nell'ambito di partiti, organismi politici, comitati di promotori e sostenitori, si possono

utilizzare senza apposito consenso dati personali relativi a iscritti e aderenti, nonché ad altri soggetti con cui si intrattengono regolari contatti. Altri enti, associazioni ed organismi senza scopo di lucro (associazioni sindacali, professionali, sportive, di categoria, *ecc.*), possono prevedere tra i propri scopi anche le finalità di propaganda elettorale che, se perseguite direttamente dai medesimi enti, organismi o associazioni, non richiedono il consenso. I dati estratti dagli elenchi telefonici possono essere invece trattati a fini di propaganda elettorale per l'invio di posta ordinaria o di chiamate telefoniche effettuate da un operatore, a seconda dei simboli apposti sull'elenco.

Qualora si ricorra all'invio di fax, di *Sms* e *Mms*, o di e-mail, nonché a chiamate telefoniche senza l'intervento di un operatore oppure a chiamate a terminali di telefonia mobile, non è possibile svolgere attività di propaganda politica senza il consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente gli scopi per i quali i dati sono utilizzati.

L'eventuale acquisizione dei dati personali da un terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, compresi quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dal verificare, anche a campione e avvalendosi del mandatario elettorale, che il terzo: a) abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda e abbia ottenuto il loro consenso idoneo ed esplicito; b) non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili. Le medesime cautele devono essere osservate anche laddove il terzo, oltre a fornire i dati, svolga le funzioni di responsabile del trattamento designato da chi effettua la propaganda.

Per quanto riguarda la casistica, è da menzionare che l'Autorità è stata interpellata dal Comune dell'Aquila a proposito delle richieste pervenute da parte delle forze politiche di acquisire, a fini di propaganda elettorale, gli elenchi in cui a seguito del sisma del 2009 sono stati registrati i nuovi indirizzi provvisori degli elettori. Tali recapiti, privi dei riferimenti telefonici, sono raccolti dal Comune medesimo in apposite banche dati, correlate alle diverse tipologie di "modalità abitative" (Moduli abitativi provvisori, Moduli

abitativi rimovibili, Progetto "Case", affitti concordati, strutture ricettive, autonoma sistemazione all'interno e al di fuori del territorio aquilano), al fine di controllare il movimento migratorio tuttora in atto.

Al riguardo, in relazione ai soli profili di competenza del Garante, non è stata ritenuta preclusa, con riferimento alle specifiche esigenze rappresentate con il quesito, la possibilità che per l'inoltro di messaggi elettorali e politici possano essere fornite, ai richiedenti legittimati, gli indirizzi provvisori dei soli cittadini iscritti nelle liste elettorali in possesso del Comune dell'Aquila, con esclusione di ogni altra informazione non pertinente (*Provv.* 4 febbraio 2010 [doc. *web* n. 1694777]).

Il provvedimento è stato trasmesso al Ministero dell'interno, per le valutazioni di competenza in relazione alle specifiche disposizioni di settore applicabili (*Nota* 11 febbraio 2010).

In un altro caso, una società aveva posto un quesito sulla possibilità di acquisire presso i comuni copia delle liste elettorali per conto di partiti, organismi politici, comitati e singoli candidati, i quali si erano rivolti alla società medesima per ottenere servizi di imbustamento, stampa e recapito, tramite il servizio postale, di comunicazioni di propaganda elettorale, comprensivi anche della gestione dei dati personali (nominativi e indirizzo) dei destinatari delle comunicazioni.

In proposito si è preso atto che i predetti soggetti, anche in maniera coordinata tra loro, nella loro qualità di titolari del trattamento dei dati contenuti nelle liste elettorali, avevano commissionato alla società, designandola a tale fine responsabile del trattamento (art. 29 del Codice), lo svolgimento delle operazioni di trattamento per la campagna elettorale e, inoltre, che la società aveva espressamente escluso la possibilità di perseguire proprie finalità autonome quale titolare del trattamento, in specie, di commercializzazione dei dati così raccolti per servizi di *marketing* diretto.

E' stato puntualizzato, comunque, che l'eventuale acquisizione dei dati personali da un soggetto terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, compresi quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dall'onere di verificare, anche

con modalità a campione e avvalendosi del mandatario elettorale, che il terzo: a) abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda elettorale e abbia ottenuto il loro consenso idoneo ed esplicito; il consenso deve risultare manifestato liberamente, in termini differenziati rispetto all'eventuale prestazione di beni e servizi e documentato per iscritto; b) non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili (artt. 11 e 61 del Codice).

In ultimo, non è stato ritenuto corretto il trattamento dei dati personali che la società intendeva effettuare a seguito della raccolta e dell'archiviazione elettronica delle liste acquisite nella qualità di responsabile del trattamento: è stato sottolineato come non risulti lecito rendere utilizzabili i dati personali così acquisiti e detenuti nei confronti di altri partiti, candidati ed organismi che ne facciano successivamente richiesta (*Nota* 24 febbraio 2010).

Associazioni

L'Autorità è stata chiamata a definire un reclamo in merito al trattamento di dati personali svolto presso un'associazione avente lo scopo di promuovere azioni di evangelizzazione e di apostolato verso individui ammalati e disabili (*Provv.* 2 aprile 2009 [doc. *web* n. 1606059]).

La reclamante, in qualità di ex associata, aveva lamentato la ricezione di una lettera dal contenuto propagandistico-elettorale inviata da un componente del consiglio direttivo dell'associazione, che avrebbe a tal fine utilizzato alcuni suoi dati personali, oltre a quelli di altri iscritti.

A seguito delle verifiche effettuate, anche di tipo ispettivo, l'Autorità ha ritenuto il trattamento dei dati personali della reclamante effettuato per finalità non compatibili con gli scopi originari della raccolta, con conseguente violazione dell'art. 11, comma 1, lett. *a*) e *b*), del Codice. Inoltre, non è risultato comprovato che fosse stata resa l'informativa all'interessata e acquisito il relativo consenso anche per finalità di propaganda elettorale.

Peraltro, in considerazione della natura dell'associazione e dei dati trattati, idonei a rivelare anche le convinzioni religiose degli interessati, l'associazione avrebbe dovuto adottare idonee e preventive misure di sicurezza, anche per prevenire eventuali rischi

di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le risultanze istruttorie hanno invece evidenziato la mancata adozione, all'epoca dei fatti contestati, di tali misure.

In particolare, non è risultato provato che l'associazione avesse all'epoca designato gli incaricati per il trattamento dei dati personali riferiti agli associati (né tale era il componente del consiglio direttivo coinvolto nella vicenda), né che avesse provveduto ad adeguati interventi formativi sul personale addetto alle operazioni di trattamento dei dati degli aderenti.

L'Autorità al riguardo ha prescritto all'associazione di adottare, in relazione all'archivio, le misure di sicurezza previste dagli artt. 31 *ss.* del Codice, e di utilizzare le informazioni contenute nell'archivio esclusivamente per finalità storiche e statistiche; è stato inoltre prescritto all'associazione di provvedere alla designazione degli incaricati del trattamento. L'Autorità ha peraltro inviato gli atti alla Procura della Repubblica per l'eventuale contestazione del reato di cui all'art. 169 del Codice.

10. LE ATTIVITÀ ECONOMICHE E I RAPPORTI DI LAVORO

10.1. SETTORE BANCARIO

Come già registrato nelle precedenti edizioni, anche nel 2009 la materia bancaria è stata oggetto di numerosi interventi dell'Autorità tesi, oltre che a ribadire l'esigenza di adottare le misure minime di sicurezza, a prescrivere il rigoroso controllo sull'attività degli incaricati nonché a sensibilizzare gli stessi al rispetto delle istruzioni ricevute.

In particolare, con una segnalazione l'interessata aveva lamentato, nell'ambito di una causa di separazione, il deposito di una memoria difensiva nell'interesse del marito, contenente informazioni bancarie a sé riferite ed asseritamente acquisite tramite un funzionario della banca.

Nell'ambito dei controlli svolti dall'Autorità, è emerso che effettivamente un dipendente della banca aveva effettuato alcune interrogazioni sui conti correnti bancari della segnalante, dando comunicazione degli esiti ad altro dipendente appartenente a una società dello stesso gruppo bancario e che detti accessi erano stati effettuati da una filiale diversa da quella nella quale il conto corrente risultava acceso.

Il Garante, con *provvedimento* del 18 giugno 2009 [doc. *web* n. 1635720], ha dichiarato illecito il trattamento di dati personali effettuato presso l'istituto di credito nelle forme della consultazione e della loro successiva comunicazione a terzi (nel caso di specie, altro dipendente dello stesso gruppo bancario) ed ha altresì prescritto al titolare del trattamento di adottare le misure di sicurezza "idonee" ad evitare accessi non autorizzati e tese a garantire la scrupolosa vigilanza sull'operato degli incaricati, nonché a sensibilizzare gli stessi incaricati al rispetto delle istruzioni ricevute anche nel corso delle iniziative formative (regola 19.6. dell'Allegato B. al Codice).

In un altro caso, la segnalante aveva lamentato una comunicazione a terzi di dati bancari a sé riferiti, successivamente utilizzati nell'ambito di un procedimento di pignoramento presso terzi. Nel corso degli accertamenti effettuati, sono stati riscontrati accessi indebiti compiuti da un terminale posto presso una filiale della banca presso la quale la segnalante era stata correntista, ma dove aveva successivamente estinto tale conto.

Tale trattamento illecito era stato peraltro possibile anche grazie all'utilizzo di una postazione erroneamente configurata (che consentiva anche a livello di filiale la visualizzazione di informazioni relative alla clientela prevista per unità organizzative di "area territoriale"): ciò in violazione degli artt. 3, 31 *ss.* del Codice, che prescrivono misure organizzative e di sicurezza finalizzate alla riduzione di accessi non autorizzati o non conformi alle finalità del trattamento.

Anche in questo caso, ritenuto che la banca avesse adottato le misure di sicurezza "minime" a protezione dei dati dei clienti trattati con l'ausilio di strumenti elettronici conformi a quanto prescritto dagli artt. 33 e 34 del Codice e dalle regole 1-26 dell'Allegato B. al Codice, il Garante ha tuttavia prescritto alla banca di adottare idonee misure organizzative, ai sensi dell'art. 31 del Codice, tese sia a garantire la scrupolosa vigilanza sull'operato degli incaricati, sia a sensibilizzare gli incaricati al rispetto delle istruzioni ricevute (*Provv.* 23 luglio 2009 [doc. *web* n. 1640294]).

In un'altra fattispecie il segnalante - socio accomandatario di una società presso la quale collaborava anche il figlio - aveva lamentato che una società emittente carte di credito, nell'ambito di un procedimento di separazione giudiziale relativa al nominato figlio, avesse dato esecuzione ad una pronuncia dell'autorità giudiziaria contenente la richiesta rivolta alla Guardia di finanza di accertare se il figlio avesse la disponibilità delle carte di credito della società, se ne avesse fatto e ne facesse utilizzo e con quale frequenza, per quali spese e per quali importi. In particolare, il segnalante aveva lamentato che la società emittente carte di credito avesse comunicato anche dati inerenti ad operazioni riferite ad una carta non intestata al figlio.

L'Autorità, pur tenendo conto delle peculiari circostanze riferite dal titolare del trattamento che avevano reso possibile l'indebita comunicazione di informazioni non pertinenti rispetto alla controversia pendente (art. 11 del Codice) e che tale trattamento aveva esaurito i suoi effetti (fatta salva ogni valutazione dell'autorità giudiziaria adita circa l'ammissibilità e la rilevanza delle prove acquisite in corso di causa) ha ritenuto di dover richiamare in ogni caso l'attenzione della società sulla necessità di una più rigorosa vigilanza sull'operato degli incaricati e sul rispetto e l'attuazione da parte dei medesimi

delle istruzioni loro impartite (*Nota* 4 dicembre 2009).

In un altro reclamo è stata lamentata l'illecita comunicazione a terzi, nella specie al padre del segnalante, di informazioni bancarie riferite al figlio. In particolare il genitore, convocato presso l'istituto bancario per il tramite della polizia municipale, era stato messo a conoscenza di una grave situazione debitoria in capo al figlio, con l'indicazione delle cifre di scoperto e del dettaglio di tutti i movimenti del conto corrente.

All'esito dell'attività istruttoria il Garante, con *provvedimento* del 28 maggio 2009 [doc. *web* n. 1624734] ha ritenuto che il comportamento tenuto dal personale della banca avesse determinato un trattamento di dati personali non previamente autorizzato dall'interessato (art. 23 del Codice) non conforme a correttezza (art. 11, comma 1, lett. *a*), del Codice). La banca, una volta acquisito il recapito telefonico dell'interessato, avrebbe dovuto mettersi in contatto solo con il figlio, e rimettere ad un'autonoma scelta di questo le successive iniziative da assumere.

Il Garante ha, inoltre, ritenuto che le modalità utilizzate dalla banca per prendere contatto con il padre del segnalante attraverso la polizia municipale fossero in violazione dell'art. 11, comma 1, lett. *a*), del Codice dal punto di vista della correttezza del trattamento, essendo per sé idonee a rendere edotti soggetti terzi (privi di titolo alcuno per operare quali ausiliari della banca) delle relazioni bancarie tra padre e figlio.

In un reclamo una società aveva rappresentato che, a seguito della cessazione dalla carica di un procuratore, aveva richiesto al proprio istituto bancario di disattivare le credenziali di autenticazione a lui assegnate per accedere *online* ai conti bancari societari. La banca tuttavia, nonostante i numerosi successivi solleciti, non aveva dato seguito alla richiesta, comunicando con ritardo l'avvenuta revoca delle credenziali del procuratore. All'esito degli accertamenti ispettivi svolti dall'Autorità il ritardo è risultato addebitabile a un errore del personale dell'agenzia. Il Garante ha pertanto richiamato la banca ad adottare le misure di sicurezza idonee a contenere il rischio di accesso non autorizzato ai sensi dell'art. 31 del Codice, ossia ad assicurare la tempestiva disattivazione delle credenziali di autenticazione attribuite alla clientela (*Provv.* 28 maggio 2009 [doc. *web* n. 1624668]).

Un segnalante aveva lamentato, da parte di una banca, l'illecita comunicazione di informazioni riguardanti suoi rapporti bancari al legale della sua controparte, che le avrebbe successivamente utilizzate nell'ambito di un procedimento giudiziario.

All'esito dell'attività istruttoria, con *nota* del 4 aprile 2009, il Garante ha rilevato in via preliminare che l'art. 160, comma 6, del Codice (in conformità, dal punto di vista sistematico, all'art. 116, primo comma c.p.c.) prevede che la valutazione della validità, efficacia e utilizzabilità di atti e documenti nell'ambito del procedimento giudiziario basati sull'illegittimo trattamento di dati personali spettano all'autorità giudiziaria.

Con specifico riferimento al caso in esame, il Garante ha ritenuto non comprovata una violazione della disciplina in materia di protezione dei dati personali - non risultando illecita la comunicazione - quando il terzo citato nell'ambito di una procedura di sequestro conservativo (nel caso di specie, la banca) rende la dichiarazione nei modi previsti dall'art. 547 c.p.c., come modificato dalla legge 24 febbraio 2006, n. 52 (*Riforma delle esecuzioni mobiliari*), tra cui rientra la comunicazione con invio di raccomandata.

Fusioni e scissioni

Considerata la ricorrenza delle operazioni societarie di fusione e di scissione e del connesso trattamento di dati personali dei soggetti interessati coinvolti, il Garante ha adottato l'8 aprile 2009 un *provvedimento* di carattere generale [doc. *web* n. 1609999] nel quale ha fornito chiarimenti circa gli adempimenti che devono essere posti in essere per rendere il trattamento conforme alla disciplina di protezione dei dati personali.

Il provvedimento, conforme alle decisioni adottate in materia nei confronti di due istituti di credito (*Provv.* 11 dicembre 2008 [doc. *web* n. 1584328] e *Provv.* 19 dicembre 2008 [doc. *web* n. 1584272]), ha stabilito che, a seguito del processo di fusione o scissione, le società coinvolte devono informare tutti i soggetti interessati (clienti, lavoratori, fornitori, *ecc.*) su chi sia il titolare e il nuovo responsabile del trattamento dei dati personali in possesso dell'impresa, al quale potersi rivolgere per esercitare il diritto di accesso e tutti gli altri diritti previsti dal Codice.

La soluzione della *"continuità"* tra i soggetti interessati dalla fusione è conforme a quella seguita dalle Sezioni unite della Corte di Cassazione (sentenza n. 2637 dell'8 febbraio 2006), in base alla quale *"la fusione tra società, prevista dagli artt. 2501 c.c. e segg.,*

non determina, nella ipotesi di fusione per incorporazione, l'estinzione della società incorporata, né crea un nuovo soggetto di diritto nell'ipotesi di fusione paritaria; ma attua l'unificazione mediante l'integrazione reciproca delle società partecipanti alla fusione. Il fenomeno non comporta, dunque, l'estinzione di un soggetto e (correlativamente) la creazione di un diverso soggetto, risolvendosi [...] in una vicenda meramente evolutiva-modificativa dello stesso soggetto, che conserva la propria identità, pur in un nuovo assetto organizzativo".

Per semplificare gli adempimenti nella fase di cambiamento societario, l'Autorità ha altresì prescritto, quale misura opportuna, l'aggiornamento dell'informativa resa dalla società scissa e dalle società partecipanti alla fusione (in particolare: la nuova denominazione del titolare del trattamento, gli estremi identificativi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali) attraverso il sito *web* delle società interessate dalle operazioni di scissione e fusione e, con comunicazione individualizzata agli interessati, in occasione della prima circostanza utile di contatto.

Nel caso in cui le società risultanti dal processo di fusione o scissione effettuino trattamenti in cui è prevista la notificazione al Garante, tali aziende dovranno effettuare o integrare la notificazione secondo le procedure *standard* previste dall'Autorità.

Comunicazioni infragruppo tra intermediari finanziari

Il Garante, a seguito di un quesito pervenuto, ha adottato il 10 settembre 2009 un *provvedimento* [doc. *web* n. 1664492] relativo alla comunicazione, tra intermediari finanziari appartenenti ad un medesimo gruppo, di dati personali relativi alle segnalazioni di operazioni considerate "sospette" ai sensi della normativa antiriciclaggio.

In particolare, all'Autorità era stato chiesto di valutare la ricorrenza, in relazione a dette comunicazioni (ivi comprese quelle verso intermediari appartenenti allo stesso gruppo stabiliti in Paesi terzi), dei presupposti per l'applicazione dell'art. 24, comma 1, lett. *g*) del Codice (relativo al *cd.* "bilanciamento di interessi").

Al riguardo occorre ricordare che sulla questione del coordinamento tra la normativa sulla protezione dei dati personali e la disciplina in materia di antiriciclaggio il Garante si era già espresso con il *parere* del 25 luglio 2007 [doc. *web* n. 1431012].

Nel *provvedimento* del 2009 il Garante ha ritenuto che, nel caso di specie, vi fossero

gli estremi per dare attuazione al principio del bilanciamento degli interessi disciplinato dall'art. 24, comma 1, lett. *g*), del Codice e che potessero, quindi, formare oggetto di comunicazione, per le esclusive finalità di contrasto al riciclaggio, i dati personali concernenti le segnalazioni previste dalla disciplina in materia di riciclaggio tra gli intermediari finanziari appartenenti al medesimo gruppo, in presenza delle condizioni previste dall'art. 46, comma 4, d.lgs. n. 231/2007, senza che a tal fine fosse quindi necessario acquisire il consenso degli interessati.

Ciò in considerazione della ponderazione tra le diverse situazioni giuridiche soggettive effettuata nel menzionato decreto legislativo, nel quale si precisa che il divieto di comunicazione a terzi della circostanza dell'avvenuta segnalazione previsto dall'art. 46, comma 1, non impedisce che essa avvenga *"tra gli intermediari finanziari appartenenti al medesimo gruppo"* (art. 46, comma 4). Ponderazione che, nel facoltizzare tale comunicazione tra gli intermediari finanziari appartenenti al medesimo gruppo, consente di non ritenere prevalenti, entro tale circoscritto ambito, i diritti degli interessati rispetto al legittimo interesse del titolare del trattamento e del terzo destinatario dei dati (nel caso di specie, altro intermediario finanziario appartenente al medesimo gruppo) alla comunicazione e al conseguente trattamento dei dati personali oggetto della segnalazione.

Di tale comunicazione, che potrà essere effettuata da parte dei soli incaricati (operanti nell'ambito dei diversi intermediari finanziari) dell'adempimento delle misure poste a contrasto del riciclaggio di denaro, il titolare dovrà fornire adeguata informativa agli interessati, dando distinte e specifiche indicazioni anche riguardo alla possibilità che le informazioni relative alle operazioni poste in essere dagli stessi interessati, ove ritenute "sospette" ai sensi dell'art. 41, comma 1, del d.lgs. 21 novembre 2007, n. 231, siano comunicate ad altri intermediari finanziari appartenenti al medesimo gruppo.

In relazione poi al trasferimento dei dati relativi alla segnalazione verso intermediari finanziari appartenenti allo stesso gruppo stabiliti in Paesi terzi, il provvedimento ha stabilito che tale trasferimento potrà avvenire ove ricorra uno dei presupposti indicati dalla legge (art. 44 del Codice).

10.2. INFORMAZIONI COMMERCIALI

Nel 2009 l'Autorità, a seguito di un'intensa attività collaborativa con l'Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito (Ancic, che controllano l'80% del volume d'affari del mercato considerato) ha affrontato la tematica dell'esonero dall'obbligo di fornire l'informativa agli interessati nell'ambito delle attività di *cd. "informazione commerciale"*.

Con il *provvedimento* del 14 maggio 2009 [doc. *web* n. 1616828] le società associate ad Ancic che operano nel settore delle informazioni commerciali sono state esonerate dall'obbligo di rendere un'informativa individualizzata in relazione al trattamento di dati personali provenienti da fonti pubbliche (o informazioni comunque pubblicamente accessibili) ove effettuato nel rispetto dei princìpi posti in materia di protezione dei dati personali. Ancic aveva rappresentato che i costi per rendere un'informativa in forma "individualizzata", risultavano sproporzionati rispetto ai diritti tutelati, in quanto elevatissimi per gli operatori di settore tenuto conto del numero ingente di soggetti ai quali la stessa avrebbe dovuto essere resa (alcuni milioni di soggetti censiti da parte di ciascuna società).

Con il medesimo provvedimento - fatte comunque salve le disposizioni contenute negli artt. 115 e 134 del r.d. 18 giugno 1931, n. 773 (*Testo unico delle leggi di pubblica sicurezza*) e la vigente normativa in materia di segreto aziendale e industriale - sono state altresì individuate misure e accorgimenti a garanzia degli interessati per consentire una maggiore conoscibilità del fenomeno delle *cd. "informazioni commerciali"* non solo tra gli operatori economici ma, più in generale, tra tutti i possibili soggetti censiti (clienti, aziende, professionisti, imprenditori, persone fisiche) dalle banche dati utilizzate per la *cd. "business information"*.

Le operazioni di trattamento prese in considerazione dal provvedimento sopra citato consistono nella raccolta e nella comunicazione alla clientela (art. 4, comma 1, lett. *l*), del Codice), anche per via telematica, di rapporti e *dossier* informativi a carattere economico o commerciale contenenti dati estratti dalle fonti pubbliche (quali visure camerali, *cd. "pregiudizievoli di conservatoria"*, dati ipocatastali, bilanci, protesti e procedure concorsuali) nonché informazioni frutto di ulteriore analisi, raffronto

ed elaborazione effettuati dalle società che rendono, in qualità di autonomi titolari del trattamento, i servizi di informazione commerciale (art. 4, comma 1, lett. *a*), del Codice).

In particolare, rispetto a tali trattamenti il Garante ha individuato, quale modalità appropriata al fine di assicurare comunque un'adeguata informativa (art. 13, comma 5, lett. *c*)) da parte delle società associate ad Ancic, la pubblicazione con cadenza annuale dell'informativa, contenente gli estremi identificativi di tutti i titolari del trattamento e gli altri elementi previsti dall'art. 13, commi 1 e 2, del Codice, sulle "Pagine Gialle" e sulle "Pagine Bianche" in versione cartacea e mediante un *banner* sui relativi siti *web*, nonché la permanente pubblicazione da parte di ciascuna delle associate ad Ancic dell'informativa prevista dall'art. 13 del Codice sul proprio sito *web*.

L'Autorità, ha inoltre stabilito, quale ulteriore misura opportuna ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, che Ancic tenga costantemente aggiornato sul proprio sito *web* l'elenco delle società di informazione commerciale alla medesima aderenti, al fine di agevolare gli interessati nell'acquisizione degli elementi dell'informativa.

10.3. SETTORE ASSICURATIVO

Si è riferito nella *Relazione 2008* (p. 133-134) sul *parere* (*Nota* del Presidente 12 febbraio 2009) relativo allo schema di regolamento sottoposto al Garante dall'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap), concernente la disciplina della banca dati antifrode (art. 135 del codice delle assicurazioni private, art. 120 del Codice) disciplinata dal provvedimento Isvap n. 2179 del 10 marzo 2003 (Banca dati sinistri r.c. auto: modalità operative per l'accesso).

10.4. RAPPORTI DI LAVORO E PREVIDENZA

10.4.1. Rapporto di lavoro in ambito pubblico

I lavoratori, nel rapporto con il proprio datore di lavoro pubblico, hanno diritto di ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (artt. 2, comma 5, e 50 d.lgs. 7 marzo 2005, n. 82, come modificato

dal d.lgs. 4 aprile 2006, n. 159). Le amministrazioni locali, pertanto, fermi gli obblighi di legge sulla trasparenza delle deliberazioni dell'ente, devono selezionare con estrema attenzione i dati personali da diffondere, non solo alla luce dei princìpi di pertinenza, non eccedenza e indispensabilità rispetto alle finalità perseguite dai singoli provvedimenti, ma anche in relazione al divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice).

Diffusione dei dati di un dipendente sul sito internet di una provincia

Lo ha ribadito il Garante accogliendo la segnalazione di una dipendente provinciale che, attraverso un motore di ricerca, aveva rinvenuto *online* alcuni atti dell'ente locale in cui erano riportati i suoi dati anagrafici e delicate informazioni sul suo stato di salute, la cui diffusione è vietata dal Codice (*Provv.* 25 giugno 2009 [doc. *web* n. 1640102]).

Richiamando le indicazioni fornite in passato agli enti locali circa l'utilizzo delle tecnologie dell'informazione (*Provv.* 19 aprile 2007 [doc. *web* n. 1407101] punto 6 e *Provv.* 14 giugno 2007 [doc. *web* n. 1417809] punto 6), l'Autorità ha ritenuto il trattamento illecito e ha disposto il blocco dei dati idonei a rivelare lo stato di salute della dipendente, contenuti in due delibere pubblicate sul sito istituzionale della provincia che, a seguito degli accertamenti effettuati dall'Ufficio, risultavano integralmente e direttamente accessibili non solo dall'*home page* del predetto sito, ma anche liberamente reperibili in internet. Le delibere, adottate del responsabile delle risorse umane dell'ente locale, riguardavano una richiesta di riconoscimento di infermità per causa di servizio avanzata dall'interessata: uno dei documenti riportava, inoltre, accanto al nome e cognome della dipendente, la valutazione medico-legale relativa al tipo di infermità riscontrata (art. 2, comma 7, d.P.R. 29 ottobre 2001, n. 461 e tab. A allegata al d.P.R. 30 dicembre 1981, n. 834; art. 6 decreto 12 febbraio 2004).

Accertamenti di idoneità al servizio: anonimato per la diagnosi Hiv

In materia di accertamenti finalizzati a verificare l'idoneità al servizio dei pubblici dipendenti, l'Autorità ha affermato che le sole informazioni che possono comparire sui certificati medici che attestano l'idoneità al servizio di un lavoratore sono quelle relative alla valutazione medico-legale (idoneità, non idoneità parziale, temporanea o permanente, con prescrizioni o limitazioni), non essendo consentito alcun riferimento alle patologie sofferte. Ciò, in particolare, nel caso di lavoratori di cui sia accertata la

sieropositività, ai quali deve essere assicurata la garanzia assoluta dell'anonimato. Questi princìpi sono stati ribaditi dal Garante con il *provvedimento* del 2 ottobre 2009 [doc. *web* n. 1658119] in cui è stato ritenuto fondato il reclamo di un dipendente del Ministero della difesa che aveva contestato la modalità con cui i suoi dati erano circolati all'interno del Ministero. Nel verbale della visita collegiale trasmesso dalla commissione medica all'Ispettorato di sanità della marina erano infatti riportati i dati nominativi dell'interessato e la diagnosi accertata. Nella copia del verbale inviata all'ufficio del personale del Ministero e al comando di appartenenza dell'interessato la diagnosi risultava invece *"sbarrata e omessa"*, consentendo così, seppure indirettamente, di risalire all'infezione da Hiv, in quanto la prassi di oscurare la diagnosi sui verbali di accertamento medico era stata adottata dall'amministrazione unicamente per la sieropositività.

Il Garante ha pertanto vietato al Ministero di utilizzare ulteriormente le informazioni sulla salute del lavoratore, specie quelle riguardanti l'Hiv, riportate nella documentazione medica. Ha inoltre prescritto di utilizzare un attestato che riporti il solo giudizio medico-legale senza diagnosi, anziché il verbale integrale della visita collegiale, in tutti i casi di accertamento sanitario di idoneità al servizio o di altre forme di inabilità. L'Autorità ha infine sollecitato l'amministrazione a modificare anche il modello di informativa utilizzato, al fine di informare in modo chiaro i lavoratori interessati sull'obbligatorietà o meno di fornire i dati sulla propria salute e sulle relative conseguenze nell'ambito degli accertamenti medico legali ai fini dell'idoneità al servizio.

In un altro caso, un'insegnante aveva contestato dinanzi all'Autorità che il circolo didattico, presso cui prestava servizio, era in possesso di copia integrale del verbale di visita medica effettuata a seguito della sua richiesta di pensione di inabilità, sul quale erano riportati informazioni riferite alla diagnosi accertata, agli esami obiettivi e agli accertamenti clinici e strumentali compiuti, nonché dati anamnestici, tra cui quelli relativi all'infezione da Hiv contratta in precedenza dall'interessata.

Dagli accertamenti effettuati nel corso dell'istruttoria l'amministrazione scolastica, tuttavia, non risultava più in possesso della documentazione medico-legale riferita alla dipendente: dopo aver ricevuto la copia del verbale di visita dalla commissione medica di

verifica del Ministero dell'economia e delle finanze, la sede di servizio dell'interessata l'aveva infatti inviata, insieme al fascicolo personale della dipendente, al circolo didattico presso cui la docente figurava come titolare, in quanto competente ad adottare i provvedimenti conseguenti all'accertata inabilità al lavoro dell'interessata.

Con il *provvedimento* del 24 dicembre 2009 [doc. *web* n. 1658058] il Garante, ritenendo illecita l'avvenuta trasmissione di copia integrale del verbale di visita da parte dall'organo di accertamento sanitario, ha vietato alla commissione medica di effettuare ulteriori comunicazioni illecite dei dati sulla salute della dipendente contenuti nella predetta documentazione. Richiamando le particolari cautele previste dalla normativa sulla protezione dei dati, nonché dalla l. n. 135/1990, per il trattamento delle informazioni sanitarie e, in particolare per quelle riguardanti l'Hiv, l'Autorità ha altresì richiesto alla commissione medica di utilizzare, in luogo del verbale integrale di visita, un attestato riportante la sola valutazione medico-legale ai fini della comunicazione alle amministrazioni di appartenenza dei lavoratori interessati dell'esito degli accertamenti sanitari di inidoneità al servizio o altre forme di inabilità non dipendenti da causa di servizio.

Nel medesimo provvedimento, avverso il quale pende un'opposizione dinanzi all'autorità giudiziaria, il Garante ha infine ritenuto illecito il trattamento dei dati sanitari della docente posto in essere dall'amministrazione scolastica presso cui prestava servizio: questa infatti, in conformità a quanto indicato dall'Autorità nelle *"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]) circa l'inutilizzabilità delle informazioni trattate in violazione della disciplina rilevante sulla protezione dei dati, avrebbe dovuto astenersi da ogni ulteriore operazione di trattamento delle informazioni dell'interessata contenute nella documentazione medica pervenuta, ad eccezione di quelle relative alla valutazione medico-legale, adottando ogni misura idonea a limitarne rigorosamente la loro conoscibilità (linee-guida *cit.*, punti 3.2 e 8.4). Ciò, senza pregiudicare la prosecuzione del procedimento avviato dall'interessata volto ad ottenere la pensione di inabilità.

In ragione dell'estrema delicatezza delle informazioni sanitarie dell'interessata riportate

nella copia integrale del verbale di visita, è stato invece vietato all'amministrazione scolastica - che ne è risultata effettivamente in possesso - di utilizzare ulteriormente tali informazioni, con conseguente obbligo di adottare ogni misura di ulteriore conservazione del documento che li contiene idonea a limitarne rigorosamente la conoscibilità, stante l'inutilizzabilità dei medesimi dati (*cfr.* artt. 11 e 22, commi 1, 3 e 5, del Codice; art. 5, l. n. 135/1990; artt. 4, 5 e 6, comma 8, del d.P.R. n. 461/2001).

Trattamenti di dati sanitari del personale del Ministero della difesa

Il soggetto pubblico datore di lavoro, nell'utilizzare per una finalità lecita i dati sensibili relativi allo stato di salute dei propri dipendenti deve, in particolare, eliminare ogni occasione di superflua conoscibilità di dati sulla salute anche da parte degli stessi soggetti incaricati o responsabili del trattamento (artt. 11, 22, commi 1, 5 e 9 e 112 del Codice) (*Provvedimenti* 23 luglio 2004 [doc. *web* n. 1099216] e 2 ottobre 2009 [doc. *web* n. 1658119] *cit.*).

Tali princìpi sono stati ribaditi dal Garante nel *provvedimento* del 21 ottobre 2009, con cui ha ritenuto fondata la segnalazione di un militare cessato dal servizio per permanente inidoneità, il quale aveva contestato la liceità del trattamento dei suoi dati personali contenuti in alcuni documenti sanitari detenuti dall'ufficio del personale del Ministero della difesa, ritenendo che tale ufficio, avente competenze non sanitarie in materia di stato giuridico, avanzamento e contenzioso del personale militare, avesse indebitamente raccolto informazioni relative al suo stato di salute attraverso l'acquisizione delle certificazioni e dei verbali di visita medica formati dagli organismi sanitari militari.

Nella specie, la documentazione trasmessa dalle commissioni mediche militari all'ufficio del personale era risultata contenere informazioni non necessarie per l'adozione dei provvedimenti di competenza in materia di stato giuridico e di avanzamento dei militari. Nel corso dell'istruttoria della segnalazione tali informazioni riguardanti, in particolare, l'anamnesi, le patologie accertate, gli esami clinici e gli altri accertamenti sanitari effettuati erano state, d'altra parte, espunte dalla documentazione posseduta a cura dello stesso ufficio del personale, in quanto ritenute eccedenti, non pertinenti e non indispensabili (artt. 11, comma 1, lett. *d*), 22, commi 3 e 5, e 112 del Codice; l. 10 aprile 1954, n. 113, sullo stato degli ufficiali dell'Esercito, della Marina e dell'Aeronautica).

Richiamando le indicazioni fornite nelle linee-guida in materia di trattamento di dati personali dei dipendenti pubblici [doc. *web* n. 1417809] citate e ferme restando le prescrizioni impartite al Ministero della difesa nel citato *provvedimento* del 2 ottobre 2009, il Garante ha pertanto richiesto all'amministrazione di rendere conformi alla normativa sulla riservatezza le modalità di circolazione interna dei dati sulla salute del personale (*Provv.* 21 ottobre 2009 [doc. *web* n. 1689440]).

Pubblicazione *online* di elenchi del collocamento obbligatorio

In materia di trattamenti di dati effettuati nell'ambito delle attività di avviamento al lavoro, il Garante, sulla base di un autonomo accertamento avviato dall'Ufficio, ha disposto il blocco della diffusione in internet dei dati sanitari di migliaia di persone iscritte nelle graduatorie, provvisorie e definitive, negli elenchi del collocamento obbligatorio dei disabili, delle categorie protette e dei centralinisti telefonici non vedenti. All'amministrazione provinciale che aveva pubblicato tali informazioni sul proprio sito istituzionale è stata contestata anche una sanzione pecuniaria per illecito trattamento dei dati sulla base dei nuovi poteri sanzionatori attribuiti al Garante dalla l. 27 febbraio 2009, n. 14, di conversione, con modificazioni, del d.l. 30 dicembre 2008 n. 207 (art. 162, comma 2-*bis*, del Codice).

Dall'accertamento svolto è emerso che nelle graduatorie - liberamente accessibili dall'*home page* del sito della Provincia - erano menzionati integralmente e senza alcuna limitazione, accanto al nominativo degli interessati, anche il codice fiscale, il comune di residenza, il reddito, nonché lo specifico stato di disabilità o di appartenenza alle altre categorie previste dalla normativa sul collocamento obbligatorio (invalido civile, invalido del lavoro, invalido di servizio, profugo, eventi terroristici, cieco assoluto, *ecc.*).

Nel provvedimento di blocco il Garante ha rilevato che l'amministrazione provinciale, nella predisposizione degli elenchi formati in attuazione della normativa sul collocamento obbligatorio, può effettuare le sole operazioni indispensabili per garantire la trasparenza delle graduatorie e il corretto svolgimento delle attività di avviamento al lavoro, astenendosi da ogni forma di diffusione di informazioni idonee a rivelare lo stato di salute (*Provv.* 21 aprile 2009 [doc. *web* n. 1616870]). Tali informazioni vanno rese conoscibili ai soggetti legittimati anche attraverso l'utilizzo di tecnologie telematiche, rispettando

il divieto di diffusione dei dati sulla salute.

Copia del provvedimento è stata inviata anche al Ministero del lavoro, della salute e delle politiche sociali e alla Conferenza Stato-Regioni affinché, nella predisposizione delle graduatorie dei disabili vengano individuate, in conformità alla legge, forme proporzionate di accessibilità ai dati in grado di contemperare il diritto alla riservatezza e la trasparenza amministrativa.

Pubblicazione *online* di dati relativi a consorzi e società di cui fanno parte le amministrazioni pubbliche

Con riferimento all'*"operazione trasparenza"* avviata dal Ministro per la pubblica amministrazione e l'innovazione, il Dipartimento per la funzione pubblica ha chiesto all'Autorità una valutazione sulla pubblicazione *online* di dati personali relativi ad incarichi ricoperti in consorzi e società di cui fanno parte le amministrazioni pubbliche. In particolare, è stato evidenziato che, tra i dati che le amministrazioni pubbliche sono tenute a comunicare al Dipartimento, ai sensi del comma 587 della legge finanziaria per il 2007 - definiti "pubblici" dal comma 591 della medesima legge - vi sono anche i nominativi e il trattamento economico lordo annuo degli incarichi ricoperti dai rappresentanti delle amministrazioni in consorzi e società. Al riguardo, l'Autorità ha condiviso la scelta del Dipartimento di non pubblicare sul proprio sito internet anche i codici fiscali di tali rappresentanti in quanto non pertinenti ed eccedenti rispetto alle finalità che si intendono perseguire con la predetta pubblicazione (*Nota* 20 aprile 2009).

Utilizzo di *test* psicoattitudinali nell'ambito di procedure concorsuali e pubblicazione su internet della relativa graduatoria

Un reclamo aveva lamentato la pubblicazione in internet della graduatoria di un concorso bandito da un comune, con le generalità dei candidati ed i risultati dei *test* psicoattitudinali utilizzati per descrivere e valutare alcuni tratti della personalità degli interessati nell'ambito della prova preselettiva. L'Ufficio, nel rilevare che l'utilizzo di strumenti telematici per finalità di trasparenza era previsto dal regolamento dell'ente locale e che la graduatoria, a seguito di un accertamento svolto, non risultava essere ancora disponibile sul *web*, ha osservato che, sebbene i risultati anche parziali, conseguiti dai candidati nei *test* espletati fossero riportati nella graduatoria preselettiva tramite formule numeriche, non poteva escludersi che le predette indicazioni consentissero - seppure in via mediata - di risalire al profilo psicologico degli interessati indicati nominativamente.

Al riguardo, è stato richiamato quanto indicato dal Garante nelle linee-guida sulla

pubblicazione di atti e documenti di enti locali in merito all'opportunità di dare attuazione al principio di pubblicità delle procedure concorsuali, nei casi in cui questa riguardi prevalentemente solo una o alcune categorie di persone, tramite forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*; numero di protocollo o altri estremi identificativi della pratica forniti dall'ente agli aventi diritto), in modo da limitare la conoscibilità di taluni dettagli soltanto agli interessati e ai controinteressati (*Provv.* 19 aprile 2007 [doc. *web* n. 1407101] punto 5) (*Nota* 21 aprile 2009).

10.4.2. Rapporto di lavoro in ambito privato

Nel corso dell'anno l'Autorità ha avuto modo di pronunciarsi ripetutamente in ordine a distinti profili relativi ai trattamenti di dati personali nella gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati.

Un caso (*Provv.* 2 aprile 2009 [doc. *web* n. 1606053]) ha riguardato il monitoraggio costante e reiterato, effettuato da una società relativamente alla navigazione internet di un proprio dipendente; monitoraggio che avrebbe comportato la contestazione di una sanzione disciplinare, contribuendo così al successivo licenziamento dell'interessato.

Le risultanze ispettive hanno evidenziato che era stato installato un *software* che registrava sistematicamente gli accessi ai siti *web* visitati dal lavoratore, senza che tuttavia ricorressero i presupposti previsti dalla disciplina di settore in tema di controlli a distanza dell'attività lavorativa (art. 4, l. 20 maggio 1970, n. 300). Benché il dipendente, al pari del restante personale, fosse stato reso edotto del divieto di navigazione in internet per motivi diversi da quelli legati all'attività lavorativa e della possibilità di controlli sulla sua postazione individuale, il trattamento effettuato dalla società è risultato illecito sia per violazione degli artt. 11, comma 1, lett. *a*) e 114, del Codice, sia perché sproporzionato rispetto alla finalità perseguita (anche tenuto conto della forma reiterata e costante con cui il monitoraggio era stato effettuato).

Alla società è stato dunque vietato l'ulteriore trattamento di dati personali relativi agli accessi a internet effettuati dal lavoratore.

In un altro caso (*Provv.* 2 ottobre 2009 [doc. *web* n. 1665170]) la dipendente di una società ha chiesto l'intervento del Garante in relazione all'asserito accesso da parte della società stessa, durante un periodo trascorso in cassa integrazione guadagni, ai dati personali memorizzati nel computer aziendale in uso all'interessata. Era stato in particolare lamentato il mancato rilascio dell'informativa da parte della società (sia in ordine alle procedure aziendali volte a garantire l'accesso ai dati dei dipendenti assenti o sospesi dal servizio, sia al correlato trattamento), sottolineando inoltre l'eccedenza del trattamento medesimo in relazione al preteso accesso a *file* di natura personale (ritenuti estranei all'attività lavorativa e, in quanto tali, non accessibili dalla società).

A seguito di una complessa istruttoria non è risultato provato che la società avesse avuto concreto accesso (per il tramite di propri incaricati) ai dati personali in parola. Peraltro, le risultanze documentali hanno evidenziato che la stessa società aveva predisposto i necessari controlli di accesso e di autenticazione e che le cartelle erano configurate per assicurare la disponibilità dei dati in caso di emergenza. Inoltre, a tutto il personale dipendente era stata rilasciata apposita informativa con indicazione, tra l'altro, della possibilità di accesso al computer per ragioni organizzative dell'attività lavorativa.

Tuttavia, dagli atti non sono risultate chiare le condizioni di accesso da parte della società ai *file* contenuti nei computer assegnati in dotazione ai dipendenti; il Garante ha pertanto prescritto alla società di fornire agli interessati una puntuale informativa al riguardo.

In una segnalazione un dipendente di una cooperativa sociale aveva lamentato, anche in ragione della possibile circolazione del documento al di fuori del contesto lavorativo, l'esplicita indicazione nel prospetto di paga di informazioni relative alla propria appartenenza alla categoria delle *"persone svantaggiate"* (di cui all'art. 4, l. 8 novembre 1991, n. 381). Le risultanze istruttorie hanno evidenziato sia che il quadro normativo non autorizzava l'indicazione dello *status*, sia l'eccedenza dei dati trattati, attesa la possibilità di raggiungere la medesima finalità di trasparenza degli elementi della retribuzione con modalità alternative, quali l'adozione di codici sostitutivi, come peraltro già indicato in precedenti pronunce dell'Autorità (*cfr. Provv.* 19 febbraio 2002 [doc. *web* n. 1063659]

e *Provv.* 31 ottobre 2007 [doc. *web* n. 1459297]). Inoltre, il *software* utilizzato - in conformità al principio di necessità di cui all'art. 3 del Codice - avrebbe dovuto essere configurato già in partenza in modo da ridurre al minimo l'utilizzo di dati personali non necessari (nel caso di specie, peraltro, particolarmente delicati).

L'Autorità (*Provv.* 18 giugno 2009 [doc. *web* n. 1640331]) ha dunque prescritto alla cooperativa l'adozione di diciture sostitutive rispetto a quella di *"lavoratore svantaggiato"*.

Il Garante si è poi occupato (*Provv.* 2 ottobre 2009 [doc. *web* n. 1666101]) di alcune segnalazioni relative ad un patronato che (per il tramite di alcune sedi locali) aveva acquisito, in assenza di uno specifico mandato, dati personali riferiti ai segnalanti stessi (prevalentemente alle anagrafiche e alla loro situazione contributiva) che sarebbero stati successivamente utilizzati nell'ambito di una procedura di mobilità che aveva interessato la società di appartenenza.

Le risultanze istruttorie (anche ispettive) hanno evidenziato che il patronato, tramite appositi collegamenti telematici con i sistemi informativi dell'Inps, aveva effettivamente acquisito detti dati (in adempimento a specifiche richieste di un rappresentante sindacale allo stesso collegato e coinvolto nella gestione delle menzionate procedure di mobilità) per finalità di individuazione dei lavoratori "licenziabili" (anche in un'ottica di tutela degli stessi). Tale acquisizione è risultata tuttavia illecita perché effettuata (ancorché da un singolo incaricato presso la sede locale del patronato) in assenza di uno specifico mandato scritto da parte degli interessati (come previsto dalla pertinente disciplina di settore, dall'art. 116 del Codice e dalle stesse disposizioni impartite dal patronato a livello centrale); inoltre, non è risultata altrimenti provata l'acquisizione del consenso degli interessati, ovvero la ricorrenza di altro presupposto di liceità del trattamento (artt. 23, 24 e 26 del Codice).

Limitatamente a detto profilo, non sono state tuttavia formulate specifiche prescrizioni nei confronti del patronato (ferma restando l'illiceità del trattamento svolto e la risarcibilità del danno eventualmente arrecato in sede giudiziaria) atteso che il trattamento è risultato in contrasto con le apposite disposizioni da questo impartite e che erano stati comunque predisposti interventi formativi anche nei confronti dell'incaricato del

trattamento coinvolto nella vicenda. Inoltre, i modelli precedentemente utilizzati per la formale designazione degli incaricati del trattamento sono risultati successivamente integrati con le esplicite istruzioni in ordine alla necessaria acquisizione, al momento della raccolta dei dati riferiti agli utenti, del mandato di assistenza e rappresentanza.

In un'ottica di semplificazione degli obblighi derivanti dalla disciplina di protezione dei dati personali, l'Autorità ha invece prescritto al patronato (in ragione della complessiva articolazione strutturale dell'istituto) di designare quali responsabili del trattamento i soggetti operanti presso le relative strutture regionali.

Il Garante si è peraltro riservato di approfondire alcuni aspetti (pur emersi in sede istruttoria) relativi all'accesso telematico garantito ai patronati da alcuni istituti previdenziali in ordine alle proprie banche dati.

In un altro caso, l'ex dirigente di una società aveva contestato alla stessa di aver indebitamente pubblicato sul proprio sito internet un comunicato stampa che, nell'informare gli operatori del settore di alcune decisioni societarie (specie di carattere organizzativo), riportava tuttavia anche informazioni relative al suo stato di salute (provocandogli in tal modo anche difficoltà nel reinserimento professionale).

Nel ritenere fondate le doglianze del segnalante (*Provv.* 16 dicembre 2009 [doc. *web* n. 1689148]) l'Autorità ha ritenuto che, diversamente da quanto sostenuto dalla società, la locuzione *"stato morbile"* utilizzata nel caso di specie risultava idonea *"rivelare lo stato di salute"* dell'interessato in quanto per sé sola in grado di palesare informazioni attinenti alla sfera sanitaria del segnalante (a prescindere, cioè, dal puntuale riferimento a specifiche patologie dello stesso).

La pubblicazione del comunicato stampa contenente tali informazioni, pertanto, integrava un'ipotesi di diffusione di dati personali idonei a rivelare lo stato di salute, vietata dal Codice (art. 26, comma 5). Il trattamento è inoltre risultato in violazione del principio di pertinenza e non eccedenza stabilito dall'art. 11, comma 1, lett. *d*), del Codice, atteso che la società avrebbe comunque potuto assicurare la trasparenza richiesta dal mercato omettendo l'indicazione, nel comunicato stampa oggetto di pubblicazione, delle condizioni di salute riferite al segnalante.

L'Autorità ha pertanto vietato alla società l'ulteriore diffusione, per il tramite del proprio sito *web*, dei dati personali del segnalante idonei a rivelare il suo stato di salute.

A fronte delle molteplici istanze pervenute (quesiti, pareri, verifiche preliminari) da parte di numerosi operatori economici sovente appartenenti a gruppi multinazionali, l'Autorità è stata inoltre chiamata ad approfondire la tematica sul fenomeno del *cd. "whistleblowing"*.

Si tratta, in sostanza, di misure organizzative appositamente predisposte da detti operatori economici (in adempimento, talora, a specifiche indicazioni provenienti dalle società capogruppo) per rendere fruibili ai soggetti operanti a vario titolo al loro interno appositi canali comunicativi per segnalare presunti illeciti (riconducibili, in particolare, a fenomeni di corruzione o frode) ascrivibili a colleghi.

All'esito degli approfondimenti condotti, l'Autorità (stante la delicatezza del tema e la sua rilevanza sociale, anche in termini di impatto sui diritti e sulle libertà fondamentali degli interessati), ha presentato il 10 dicembre 2009 una segnalazione al Parlamento e al Governo [doc. *web* n. 1693019] indicando le ragioni che potrebbero giustificare un eventuale intervento normativo in materia.

Preliminarmente si è evidenziato che la tematica in esame è stata oggetto di attenzione da parte del Gruppo Art. 29 che, con parere del 1° febbraio 2006 (WP 117 [doc. *web* n. 1607645]), ha fornito alcune indicazioni per rendere i trattamenti di dati personali effettuati per il tramite dei menzionati sistemi di segnalazione conformi ai princìpi contenuti nella suddetta direttiva (con particolare riferimento al loro ambito di applicazione; ai presupposti di liceità del trattamento; all'esercizio del diritto di accesso da parte degli interessati; all'ammissibilità di denunce anonime).

I riferimenti normativi rinvenibili nell'ordinamento italiano (d.lgs. n. 231/2001, artt. 2105, 1175 e 1275 c.c., art. 21 Cost.) non consentono di inquadrare sistematicamente il fenomeno; peraltro, un eventuale intervento del Garante in materia, oltre a comportare scelte di più opportuna pertinenza parlamentare, si sarebbe rivelato necessariamente parziale e limitato e non avrebbe risolto i profili di criticità che il fenomeno in questione comporta in rapporto alla vigente normativa sulla protezione dei dati personali. Ciò, con particolare riferimento a:

- i presupposti di liceità del trattamento (non potendo al riguardo ravvisarsi un trattamento di dati personali riconducibile ad un obbligo legale e tenuto conto che l'alternativa percorribile - il *cd.* "bilanciamento di interessi" - avrebbe comportato un'inevitabile perimetrazione dell'ambito di applicazione dei sistemi di segnalazione, con conseguente esclusione di talune tipologie di trattamento);
- l'estensione del diritto di accesso (con particolare riferimento al diritto, da parte del soggetto segnalato, di conoscere l'origine dei dati e, segnatamente, quelli identificativi dell'autore della segnalazione) il cui esercizio potrebbe infirmare l'efficacia di tali sistemi, dissuadendo i segnalanti dal proprio intento di riferire i presunti illeciti;
- l'ammissibilità di eventuali segnalazioni *"anonime"*, suscettibili di usi strumentali e inidonee, in taluni casi, a consentire la raccolta di informazioni ulteriori. Il Garante ha quindi auspicato un intervento legislativo volto ad assicurare un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di trasparenza e di tutela delle aziende presso le quali queste operano, in particolare segnalando al Parlamento e al Governo, l'opportunità di:
  - individuare i presupposti di liceità del trattamento e l'ambito soggettivo di applicazione dell'eventuale disciplina;
  - individuare i soggetti che possono assumere la qualità di *"segnalati"*;
  - individuare le finalità perseguibili e le fattispecie oggetto di possibile *"denuncia"*;
  - definire la portata del diritto di accesso previsto dall'art. 7 del Codice;
  - stabilire l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

Un'altra pronuncia dell'Autorità ha riguardato il reclamo del dipendente di una società controllata dal Ministero per i beni e le attività culturali, relativo ad asserite violazioni del Codice da parte del datore di lavoro, in particolare con riguardo alle disposizioni in materia di misure (anche minime) di sicurezza. Più precisamente, il reclamante aveva lamentato la diffusione tra i dipendenti della società, anche a mezzo fax, del contenuto

di un verbale di conciliazione di una vertenza di lavoro sottoscritto dall'interessato in sede giudiziale. A sostegno della propria posizione, tra la documentazione allegata, il reclamante aveva prodotto la fotocopia di un fax inviato da un'utenza facente capo ad una delle sedi della società.

L'Autorità non ha ritenuto di dover adottare un provvedimento collegiale sul caso di specie, poiché dalla documentazione in atti e dalle dichiarazioni rese (anche in sede ispettiva) dalla società, era emerso che il fax, pur inviato da un'utenza della società, non conteneva informazioni che consentissero di risalire al destinatario; né è stato possibile comprovare che la trasmissione del fax fosse stata effettuata da un incaricato della società. Inoltre, i fatti riferiti al reclamante erano risultati già conoscibili da una precedente comunicazione sindacale relativa alla vicenda, pure inoltrata via fax.

Le risultanze istruttorie di accertamenti *in loco* avevano inoltre evidenziato che la società aveva adottato misure di sicurezza in conformità alle prescrizioni contenute negli artt. 31 *ss.* del Codice e nelle regole dell'Allegato B. al Codice medesimo (*Nota* 14 maggio 2009).

In un altro caso, una lavoratrice aveva lamentato l'illecita comunicazione, da parte del suo pregresso datore di lavoro, di dati personali relativi alle proprie condizioni di salute ad altra società, presso la quale la segnalante aveva pure prestato, in precedenza, la propria opera e nei confronti della quale pendeva un giudizio relativo al rapporto di lavoro cessato.

La documentazione trasmessa da una società all'altra (consistente nella richiesta di tentativo di conciliazione e nel ricorso promosso dalla segnalante ai sensi dell'art. 414 c.p.c., contenente anche dati riferiti alle condizioni di salute dell'interessata), in seguito alla comunicazione al precedente ex datore, era stata depositata da quest'ultimo anche in un diverso procedimento pendente tra il medesimo e l'interessata.

Il Garante ha rilevato che la comunicazione dei dati sensibili riferiti alla segnalante, finalizzata alla sola difesa giudiziaria della società destinataria dei dati (art. 24, comma 1, lett. *f*) e 26, comma 4, lett. *c*), del Codice) non era stata effettuata lecitamente (artt. 11 e 26, comma 4, lett. *c*), del Codice). Ciò in quanto le informazioni di natura sensibile,

in assenza di consenso dell'interessato, possono formare oggetto di comunicazione se ciò sia indispensabile per far valere o difendere un diritto in sede giudiziaria che, con particolare riferimento ai dati *"idonei a rivelare lo stato di salute e la vita sessuale"*, deve essere di rango almeno pari a quello dell'interessato, ovvero consistere in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 26, comma 4, lett. *c*)), del Codice, *autorizzazione* n. 1 al trattamento dei dati sensibili nei rapporti di lavoro 16 dicembre 2009, punto 3, lett. *d*) [doc. *web* n. 1682123]).

Nel caso di specie, invece, erano stati fatti valere solo diritti a contenuto patrimoniale connessi alla cessazione del rapporto di lavoro.

Il Garante ha pertanto vietato alla società oggetto di segnalazione ulteriori comunicazioni alla seconda società di dati riferiti alle condizioni di salute della segnalante (*Provv.* 2 aprile 2009 [doc. *web* n.1605667]).

10.4.3. Previdenza

Sistema informativo dell'Inps

Nel quadro della messa in sicurezza delle banche dati pubbliche di grande rilevanza, è stata avviata una specifica attività di controllo sul sistema informativo dell'Inps riguardo alla struttura degli archivi, alla tipologia delle informazioni raccolte, alle modalità con le quali vengono trattate all'interno dell'amministrazione e agli accessi da parte di soggetti esterni a tali informazioni, talora di carattere sensibile.

Dati personali relativi all'anzianità contributiva

Sono stati inviati chiarimenti all'Inps in ordine alla possibilità di comunicare, alle pubbliche amministrazioni che lo richiedano, i dati personali relativi all'anzianità contributiva maturata dai propri assicurati per consentire ai datori di lavoro pubblici di verificare la veridicità delle dichiarazioni rese dal personale ai fini dell'eventuale risoluzione del rapporto di lavoro, in conformità a quanto previsto dall'art. 72, comma 11, del d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, in legge 6 agosto 2008, n. 133.

Nelle more di un intervento legislativo al riguardo, è stato chiarito che le amministrazioni interessate possono avvalersi della disciplina prevista dal Testo unico delle disposizioni in materia di documentazione amministrativa (artt. 71, d.P.R. 28 dicembre 2000,

n. 445 e 19, comma 3, del Codice) (*Nota* 22 maggio 2009).

Trasferimento di atti d'archivio

In linea con quanto già affermato in passato sul tema (*Note* 14 maggio 1999 [doc. *web* n. 39288] e 13 maggio 1998 [doc. *web* n. 40053]) è stato fatto presente ad un ufficio territoriale dell'Inps che il trasferimento di atti d'archivio non presuppone specifici adempimenti nei confronti dell'Autorità, poiché la disciplina sulla protezione dei dati personali non reca alcuna modifica delle vigenti disposizioni in materia di scarto e trasferimento di atti di archivi pubblici contenute ora nel Codice in materia dei beni culturali e del paesaggio (d.lgs. 22 gennaio 2004, n. 42), che ha peraltro abrogato quanto previsto dal d.l. 29 ottobre 1999, n. 490 (art. 184 d.lgs. n. 42/2004).

In particolare, è stato precisato che le ipotesi di cessazione del trattamento, disciplinate dall'art. 16 del Codice, riguardano i casi in cui il titolare intenda interrompere in via definitiva l'intero complesso di operazioni concernenti un determinato trattamento di dati personali, non il mero scarto o trasferimento di atti d'archivio (*Nota* 25 agosto 2009).

Accesso dall'Inps alla banca dati dei sinistri

È stata sottoposto all'Autorità uno schema di convenzione volta a consentire all'Inps, pur in assenza di un'espressa previsione di legge o di regolamento, di accedere alla banca dati dei sinistri dell'Isvap prevista dall'art. 135 del Codice sulle assicurazioni private (d.lgs. 7 settembre 2005, n. 209), al fine di agevolare l'esercizio del diritto di surrogazione dell'ente previdenziale nei diritti degli assicurati danneggiati per fatti illeciti di terzi, nonché di contrastare eventuali comportamenti scorretti degli stessi assicurati.

Al riguardo, sono state evidenziate specifiche perplessità in ordine all'applicabilità della speciale disciplina dettata dall'art. 39 del Codice, alla luce delle limitazioni all'accesso alla stessa banca dati prescritte dalla normativa sulle assicurazioni private, nonché alla pertinenza e non eccedenza dei dati oggetto della prefigurata consultazione (art. 135 d.lgs. n. 209/2005 e art. 120 d.lgs. n. 196/2003; *v.* anche provvedimento Isvap n. 2179 del 10 marzo 2003 e artt. 9, 10 e 12 del nuovo schema di regolamento concernente la disciplina della banca dati sinistri di cui al documento in consultazione Isvap n. 33/2009) (*Nota* 20 maggio 2009).

Raccolta di dati relativi alla natura dell'*handicap* e cumulo dei benefici per l'assistenza a familiari disabili

L'Inps ha rappresentato all'Autorità di aver necessità di acquisire la documentazione sanitaria relativa alla natura dell'*handicap* in occasione di specifiche istanze di lavoratori, volte a ottenere il cumulo dei benefici previsti dalla l. n. 104/1992 per assistere più disabili presenti nel proprio nucleo familiare, al fine di consentire ai medici dell'ente di valutarne i presupposti alla luce del quadro normativo applicabile e dell'orientamento espresso in materia dal Consiglio di Stato (art. 33, comma 3, l. n. 104/1992 e parere n. 785/1995 del 14 giugno 1995). Al riguardo, in linea con le indicazioni fornite dal Garante nelle *"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]), l'Ufficio ha sollecitato l'Istituto ad individuare idonei accorgimenti volti a limitare la conoscibilità dei dati personali contenuti nella predetta documentazione, dovendo ritenersi preclusa anche in tali occasioni ogni loro conoscibilità da parte del soggetto pubblico datore di lavoro (*ad es.*, previsione della busta chiusa per la presentazione della documentazione sanitaria o ricorso a comunicazioni telematiche individuali con i lavoratori interessati) (*Nota* 17 aprile 2009).

Banca dei percettori

Su richiesta dell'Inps, il Garante ha consentito alle regioni e alle province autonome, pur in assenza di un'espressa previsione di legge o di regolamento, di avere accesso alla banca dati dell'Inps che raccoglie le informazioni di lavoratori e disoccupati che usufruiscono di misure di sostegno al reddito istituita ai sensi dell'art. 19, comma 4, d.l. n. 185/2008 convertito, con modificazioni in l. n. 2/2009 (*Provv.* 7 ottobre 2009 [doc. *web* n. 1658413]). La consultazione della banca dati è stata, infatti, ritenuta necessaria per consentire alle amministrazioni regionali di svolgere le proprie funzioni istituzionali in materia di politiche attive del lavoro nei riguardi dei residenti da reinserire nel mercato e, in particolare, per programmare e realizzare corsi di formazione e riqualificazione professionale, nonché per ottenere il rimborso dalla Commissione europea che cofinanzia tali interventi (artt. 19, comma 2 e 39, comma 1, lett. *a*), del Codice).

I dati personali oggetto di consultazione (anagrafici, indennità percepite, rapporto di lavoro, *ecc.*) sono risultati, inoltre, rispettosi dei princìpi di pertinenza e non eccedenza in rapporto alle finalità perseguite dagli enti regionali di avviamento al lavoro e di

formazione professionale, nonché di rendicontazione del sostegno economico erogato.

L'Autorità ha comunque richiesto all'Inps l'adozione di specifiche cautele a protezione dei dati personali. In primo luogo, in ottemperanza ai princìpi di proporzionalità, pertinenza e non eccedenza, l'Inps dovrà assicurare un accesso selettivo alle informazioni individuate ed il loro utilizzo proporzionato rispetto alle finalità perseguite in relazione allo specifico ruolo istituzionale svolto, nonché agli ambiti territoriali di competenza (art. 11 del Codice). In secondo luogo, in considerazione della temporaneità della compartecipazione regionale alle misure di sostegno al reddito, l'Istituto dovrà individuare un termine entro il quale disabilitare l'accesso alla banca dati una volta che regioni e province autonome abbiano esaurito i loro compiti in materia di gestione e attuazione degli interventi formativi e di rendicontazione a livello europeo (*v.* accordo fra Governo, regioni e province autonome del 12 febbraio 2009). Sotto il profilo della sicurezza dei dati, infine, fermo restando il rispetto delle misure minime previste dal Codice (artt. 33 *ss.* e relativo Disciplinare tecnico), occorre che l'Inps predisponga strumenti e procedure per rafforzare il meccanismo di autorizzazione e autenticazione di soggetti abilitati ad accedere alla banca dati e per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso alla stessa.

Scambio di dati relativi ai certificati medici tra Inps e Inpdap

Le recenti disposizioni in materia di pubblico impiego hanno previsto che, in tutti i casi di assenza per malattia, la certificazione medica debba essere inviata per via telematica direttamente dal medico o dalla struttura sanitaria che la rilascia all'Inps, e da questo immediatamente inoltrata all'amministrazione di appartenenza del lavoratore (art. 69, comma 1, d.lgs. 27 ottobre 2009, n. 150 che ha inserito l'art. 55-*septies* dopo l'art. 55 del d.lgs. n. 165/2001). Per poter procedere all'invio dei certificati medici alle amministrazioni interessate, l'Inps ha rappresentato al Garante, ai sensi degli artt. 19 e 39 del Codice, l'esigenza di acquisire presso l'Inpdap, attraverso il codice fiscale dei dipendenti pubblici, gli estremi identificativi delle amministrazioni di dipendenza e/o di servizio, in quanto manca una norma di legge o di regolamento che preveda questo flusso di informazioni. Al riguardo, l'Autorità ha ritenuto lo scambio di dati tra i due Enti previdenziali indispensabile per assicurare lo svolgimento dei compiti istituzionali dell'Istituto in

materia di controlli sulle assenze dei soggetti pubblici interessati (*Provv.* 8 gennaio 2010 [doc. *web* n. 1693889]). È stato comunque prescritto ai due enti di assicurare l'accesso selettivo alle sole informazioni pertinenti e non eccedenti (denominazione, codice fiscale e indirizzo dell'amministrazione di appartenenza e/o della sede di servizio) e di garantire il loro utilizzo proporzionato rispetto alle finalità perseguite (art. 11 del Codice). L'Inps e Inpdap, inoltre, fermo restando il rispetto delle misure minime di sicurezza previste dal Codice, dovranno individuare strumenti e misure organizzative per garantire un'adeguata protezione dei dati definendo, in particolare, rigorose procedure per l'autenticazione e le autorizzazioni degli utenti deputati alla consultazione. Al riguardo, i medesimi enti dovranno stipulare una convenzione atta a circoscrivere le finalità per le quali viene consentito questo esclusivo trattamento dei dati e a definire i vincoli per assicurarne la correttezza, nonché i meccanismi di autenticazione e autorizzazione, ivi incluse le soglie relative al numero di utenti abilitabili dall'Inps. In ogni caso, l'Istituto non dovrà realizzare autonome banche dati con le informazioni ricevute dall'Inpdap, vietando ai propri incaricati l'utilizzo di dispositivi automatici che consentano di consultare in forma massiva dati e di replicare la banca dati acceduta.

Per quanto riguarda, invece, la successiva trasmissione dei certificati medici da parte dell'Inps alle amministrazioni interessate, l'Autorità ha ricordato che questi non dovranno contenere l'indicazione della diagnosi, in conformità all'art. 1, comma 149, della legge 30 dicembre 2004, n. 311 e all'art. 2, comma 2, del d.l. 30 dicembre 1979, n. 663, convertito, con modificazioni, dalla legge 29 febbraio 1980, n. 33.

10.5. ALTRE ATTIVITÀ IMPRENDITORIALI

Con riferimento al tema del consenso al trattamento di dati personali sensibili (art. 26 del Codice), l'Autorità è stata chiamata a esaminare un reclamo formulato nei confronti di una società specializzata in trattamenti cosmetricologici (*Provv.* 26 febbraio 2009 [doc. *web* n. 1601558]). Il reclamante, nel contestare la validità di un contratto sottoscritto con detta società perché stipulato in ragione di una patologia del capello diagnosticata da quest'ultima e successivamente valutata inesistente da altro medico specialista interpel-

lato dall'interessato, aveva eccepito l'inidoneità dell'informativa resa in sede contrattuale e la mancata acquisizione del consenso scritto al trattamento dei propri dati personali sensibili (in quanto attinenti allo stato di salute connesso alla crescita dei capelli). Secondo il reclamante, infatti, non poteva essere qualificata come manifestazione del consenso al trattamento la mera sottoscrizione del contratto da parte dello stesso, tenuto peraltro conto che le medesime condizioni contrattuali non ne prevedevano l'espressa acquisizione (in quanto il trattamento sarebbe stato necessario per l'esecuzione degli obblighi derivanti dal contratto sottoscritto dall'interessato). La società aveva replicato sostenendo di aver lecitamente trattato i dati personali riferiti al reclamante trovando, a suo dire, applicazione nel caso di specie l'esimente di cui all'art. 24, comma 1, lett. *b*), del Codice.

L'Autorità ha ritenuto fondate le doglianze del reclamante, muovendo dall'assunto che le informazioni inerenti alle condizioni dei capelli e del cuoio capelluto (in quanto potenzialmente idonee a fornire notizie in ordine anche allo stato di salute dell'interessato: presenza di eventuali alterazioni; livelli ormonali presenti nell'individuo) fossero "dati sensibili" ai sensi dell'art. 4, comma 1, lett. *d*), del Codice, anche alla luce delle tecniche diagnostiche impiegate dalla società, che permettevano di avere un quadro complessivo non solo sullo stato di salute del capello, ma, più in generale, della cute stessa. Nel merito, è stata riscontrata l'inidoneità dell'informativa resa all'interessato (limitatamente alle informazioni concernenti i soggetti esterni che potevano venire a conoscenza dei dati e ai diritti esercitabili in base all'art. 7 del Codice), oltre alla mancata acquisizione dell'apposito consenso scritto del reclamante per il trattamento dei suoi dati sensibili. Inoltre, le risultanze documentali hanno evidenziato che all'epoca dei fatti il collaboratore esterno addetto all'attività di analisi e di laboratorio per conto della società non era stato designato responsabile del trattamento (con conseguente comunicazione a terzi, nel caso di specie, dei dati personali riferiti al reclamante).

L'Autorità, accertata quindi l'illiceità del trattamento svolto, ha prescritto alla società (anche a vantaggio della relativa clientela) di riformulare il modello di sottoscrizione concernente il contratto di fornitura dei servizi, con specifico riferimento all'informativa e

alla manifestazione del consenso al trattamento dei dati sensibili, in conformità agli artt. 13 e 26 del Codice. Il Garante ha inoltre trasmesso gli atti all'autorità giudiziaria per la valutazione di eventuali profili di violazione dell'art. 168 del Codice, in relazione all'alterazione materiale di documentazione istruttoria.

Un'altra pronuncia (*Provv.* 23 luglio 2009 [doc. *web* n. 1640398]) ha riguardato una segnalazione anonima con cui è stata lamentata la comunicazione - da parte di un'importante compagnia aerea ad altre compagnie - di dati personali sensibili riferiti alla clientela.

Dagli accertamenti ispettivi svolti presso la sede italiana della compagnia, non è risultata provata la comunicazione a terzi di detti dati; nondimeno, è stato evidenziato che la compagnia raccoglieva, nell'ambito di uno specifico programma di fidelizzazione, alcuni dati personali riferiti alla clientela, taluni dei quali anche sensibili (avuto riguardo alle preferenze alimentari degli interessati, anche in relazione alle loro condizioni di salute o alla fede religiosa professata).

Tali informazioni (acquisite per il tramite di *coupon* prestampati presso la casa madre e contenenti anche l'informativa al trattamento dei dati personali) sarebbero state trattate presso le biglietterie italiane limitatamente ai dati anagrafici (con conseguente riconducibilità della titolarità del trattamento in esame anche in capo alla sede italiana della compagnia); i dati sensibili, per contro, sarebbero stati raccolti solo a bordo degli aerei. I dati acquisiti, inoltre, sarebbero stati successivamente trasferiti all'estero, presso la sede principale della compagnia.

Dalla documentazione acquisita, l'informativa resa dalla sede italiana della compagnia alla clientela è risultata inidonea, poiché essa si limitava a rendere noto agli interessati che attraverso l'adesione al programma di fidelizzazione si autorizzava la compagnia all'utilizzo di ogni informazione acquisita per finalità commerciali o di comunicazione. L'Autorità ha dunque prescritto alla sede italiana della compagnia di riformulare l'informativa resa alla clientela nell'ambito del menzionato programma di fidelizzazione (anche con modalità alternative al suo rilascio per il tramite del citato *coupon*), limitatamente al trattamento effettuato presso le biglietterie site nel territorio dello stato italiano.

Non è risultata invece necessaria, relativamente al trasferimento dei predetti dati verso

Paesi non appartenenti all'Unione europea, la manifestazione del consenso da parte degli interessati, essendo il trattamento necessario per l'esecuzione di obblighi contrattuali (art. 43, comma 1, lett. *b*), del Codice).

L'Autorità è stata altresì chiamata a definire un reclamo avente ad oggetto una comunicazione a terzi di dati personali relativi ad un'esposizione debitoria (*Provv.* 28 maggio 2009 [doc. *web* n. 1624760]).

I reclamanti avevano sospeso i pagamenti nei confronti della società con cui era stato stipulato un contratto di appalto a seguito di asserite inadempienze da parte di quest'ultima; a fronte del mancato pagamento del corrispettivo convenuto, la società aveva inviato loro una lettera (indirizzata anche al comando aeronavale della Guardia di finanza presso cui operava uno dei reclamanti) comunicando l'intenzione di porre all'incasso, a parziale saldo del debito maturato, gli effetti cambiari sottoscritti da uno degli interessati (oltre che dal padre dell'altro) e rendendo così nota a terzi (estranei al rapporto contrattuale intercorso con la società) la loro complessiva esposizione debitoria. I reclamanti, anche in ragione di alcuni successivi colloqui del rappresentante legale della società con esponenti del predetto comando aeronavale, hanno richiesto l'intervento dell'Autorità per veder tutelate le proprie ragioni.

Dagli accertamenti ispettivi espletati è risultato che la comunicazione delle informazioni contenute nella nota inviata anche al comando aeronavale era effettuata in violazione della disciplina di protezione dei dati personali, poiché in assenza di una finalità legittima e del necessario consenso, e in contrasto con il principio di pertinenza e non eccedenza delle informazioni trattate (art. 11, comma 1, lett. *a*), *b*) e *d*), e art. 23 del Codice). Parimenti illecita è risultata la comunicazione di informazioni nei colloqui con il comandante del citato comando aeronavale, in quanto effettuata (peraltro in assenza del consenso degli interessati) per finalità e con modalità non rispettose della disciplina in materia di protezione dei dati personali. L'Autorità ha conseguentemente vietato l'ulteriore comunicazione - a terzi non aventi titolo - di dati personali relativi alla situazione debitoria degli interessati.

Un'altra pronuncia (*Provv.* 12 novembre 2009 [doc. *web* n. 1679779], *cfr. par.* 8.3.)

ha riguardato il trattamento di dati personali effettuato da un centro dentistico relativamente all'immagine di una persona nota. La segnalante aveva lamentato la pubblicazione, senza il suo consenso, di una sua fotografia su alcuni volantini pubblicitari utilizzati dal medesimo centro. Dopo aver reiteratamente (e inutilmente) diffidato il centro dentistico dall'utilizzo della sua immagine, la segnalante si è rivolta all'Autorità per ottenere la cessazione del trattamento.

Il trattamento è risultato in violazione delle disposizioni di cui all'art. 10 c.c. (in tema di *"Abuso dell'immagine altrui"*) e agli artt. 96 e 97 della legge 22 aprile 1941, n. 633 (recante *"Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"*), non ricorrendo le finalità di pubblica informazione richieste da dette disposizioni (secondo la prevalente interpretazione giurisprudenziale) per riprodurre e pubblicare con finalità commerciali il ritratto dell'interessata in difetto del relativo consenso. Inoltre, il trattamento è risultato in violazione del principio di finalità (art. 11, comma 1, lett. *b*), del Codice), oltre che degli artt. 23 e 24 del Codice (non risultando acquisito il consenso dell'interessata alla riproduzione e alla messa in commercio del proprio ritratto, come pure al relativo trattamento di dati personali).

L'Autorità ha quindi vietato al centro dentistico l'ulteriore trattamento dei dati personali riferiti all'interessata a mezzo della diffusione degli anzidetti volantini pubblicitari, fatta salva la possibilità di compiere le sole operazioni di trattamento necessarie in relazione all'eventuale tutela dei diritti in sede giudiziaria da parte dell'interessata, nonché per l'esercizio del diritto di difesa ad opera dello stesso titolare (art. 24, comma 1 lett. *f*), del Codice).

10.6. ATTIVITÀ DI IMPRESA E CONTROLLI

Il Garante si è pronunciato (*Provv.* 28 maggio 2009 [doc. *web* n. 1625257]) sul trattamento di dati personali effettuato da un importante gruppo societario (produttore di abbigliamento per bambini e *pre-maman*), mediante un sistema informatico installato presso punti vendita con i quali la società intrattiene rapporti di collaborazione commerciale non riconducibili ad un'unica fattispecie contrattuale. In base alle dichiarazioni

rese dai segnalanti, con tale sistema sarebbero stati comunicati alla società dati personali riferiti sia alla commercializzazione dei prodotti (prezzo, articolo, quantità di capi, venduti), sia ai clienti titolari della *"fidelity card"* (in particolare, informazioni anagrafiche, recapiti telefonici, indirizzi, anche e-mail e dati anagrafici dei componenti il nucleo familiare).

In relazione alla lamentata assenza del consenso a tali comunicazioni, il Garante ha stabilito che le informazioni oggetto del menzionato trattamento dovessero ritenersi, ai sensi dell'art. 11 del Codice, pertinenti e non eccedenti rispetto alle legittime finalità perseguite dalla società (*ad es.*, per programmare la produzione o rendere più efficiente la distribuzione e l'assortimento dei propri prodotti).

Ha altresì ritenuto che - avendo l'utilizzo di tale sistema formato oggetto di espressa pattuizione tra le parti - il trattamento delle informazioni personali connesse all'esecuzione di tale accordo non richiedesse il consenso degli interessati, dovendosi piuttosto invocare l'esistenza del presupposto di liceità alternativo al consenso di cui all'art. 24, comma 1, lett. *b*), del Codice. Più in generale, l'Autorità ha ritenuto che il consenso all'utilizzo dello strumento e conseguentemente alla comunicazione delle informazioni fosse desumibile dalle numerose comunicazioni elettroniche che i segnalanti avevano scambiato con la società in ordine al regolare funzionamento del sistema medesimo.

In ogni caso, l'invio dei dati non poteva avvenire automaticamente, presupponendo un'autonoma iniziativa dei titolari degli esercizi commerciali che, con cadenza giornaliera, avrebbero dovuto provvedere - attivando un'apposita procedura - a trasmetterli alla società. E' stato altresì sottolineato, che la documentazione contrattuale sottoscritta dai segnalanti conteneva la manifestazione del consenso al trattamento dei propri dati personali da parte della società. Tuttavia, rilevata l'inidoneità dell'informativa fornita a uno dei segnalanti, il Garante si è riservato di contestare la violazione, con autonomo procedimento, ai fini dell'applicazione della prevista sanzione amministrativa

Preso atto, peraltro, che il nuovo modello di informativa predisposto dalla società successivamente all'apertura dell'istruttoria risultava conforme al Codice, non si è ritenuto necessario impartire prescrizioni al riguardo.

In merito al trattamento di dati personali contenuti nelle carte di fidelizzazione, rilevato che il modello di raccolta dati conteneva informazioni eccedenti rispetto alla finalità in concreto perseguita (in particolare la professione del soggetto richiedente la carta, i dati riferiti ai figli del richiedente), è stato prescritto alla società di cancellare tali dati. Anche in tale caso, preso atto che, successivamente all'apertura dell'istruttoria da parte dell'Autorità, la società aveva riformulato il modello, non si sono rese necessarie ulteriori prescrizioni al riguardo, salvo precisare per quali dati il conferimento fosse obbligatorio.

In un altro caso, alcuni segnalanti avevano rappresentato di essere stati contattati da un procacciatore di affari nell'interesse di una società per l'acquisto di *"punti vacanza"* che consentivano all'acquirente l'utilizzo, per un determinato periodo di tempo, di alloggi siti in complessi immobiliari ubicati fuori dal territorio italiano ed amministrati da una società fiduciaria inglese (*trustee*), in nome e per conto della quale aveva agito la società oggetto di segnalazione. Il contratto proposto ai segnalanti prevedeva altresì la possibilità di un finanziamento tramite un'altra società.

I segnalanti avevano, pertanto, sottoscritto taluni contratti di compravendita di *"punti vacanze"* e relative contestuali richieste di finanziamento; per parte sua, il procacciatore di affari si era impegnato ad inviare un documento informativo da considerarsi parte integrante del contratto. Non rispettato l'impegno e subentrato un contenzioso circa la validità dei contratti stipulati, gli interessati avevano lamentato che nei contratti conclusi con la società non sarebbe stata fornita idonea informativa e che non sarebbe stato definito a che titolo il procacciatore di affari, non vincolato da rapporto di lavoro subordinato con nessuna delle due società sopra citate, avesse trattato i dati personali riferiti ai segnalanti.

All'esito dell'istruttoria (integrata con elementi acquisiti anche con un accertamento *in loco* presso la sede della società), l'Autorità ha ritenuta inidonea l'informativa resa (che indicava i soli scopi del trattamento, ma non la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze del loro mancato rilascio, né i soggetti o le categorie di soggetti ai quali i dati potevano essere comunicati e l'ambito di diffusione dei dati stessi) contestando la relativa violazione e prescrivendo alla società, in qualità di titolare del trattamento posto in essere nei confronti dei segnalanti, in particolare l'integrazione

dell'informativa con tutti gli elementi previsti dall'art. 13 del Codice (*Provv.* 4 giugno 2009 [doc. *web* n. 1630006]).

Inoltre, non è risultata comprovata la designazione del procacciatore d'affari quale incaricato del trattamento da parte della società, né alcun elemento in ordine alle istruzioni impartite circa i trattamenti effettuati dalla società e alle modalità di esercizio della sorveglianza del titolare e/o del responsabile sul rispetto delle disposizioni impartite. Il Garante ha, pertanto, prescritto alla società di adottare ogni misura organizzativa idonea per la designazione dei procacciatori di affari di cui si serve in qualità di incaricati del trattamento.

Da ultimo, in ordine all'asserita inosservanza da parte della società della normativa sul trasferimento dei dati personali all'estero - per l'assenza di uno specifico consenso dei segnalanti - la disciplina di protezione dei dati personali non è risultata violata, atteso che il consenso degli interessati non è risultato necessario ai sensi dell'art. 28, comma 4, lett. *b*), della l. n. 675/1996 (ora, art. 43, comma 1, lett. *b*), del Codice).

Con numerose segnalazioni, sono stati portati all'attenzione del Garante disservizi nell'espletamento dell'attività di recapito della corrispondenza da parte di Poste italiane S.p.A., con particolare riguardo alla consegna ad indirizzi o in cassette domiciliari erronee, nonché all'abbandono, smarrimento o danneggiamento della posta.

Sono stati pertanto acquisiti elementi volti ad accertare la conformità al Codice dei trattamenti di dati personali posti in essere dalla società, con particolare riferimento alla corretta designazione degli incaricati e di eventuali responsabili del trattamento, e all'osservanza delle misure di sicurezza anche nella fase della distruzione della corrispondenza per la quale non risulti possibile il recapito.

Con *provvedimento* 29 aprile 2009 [doc. *web* n. 1617709] il Garante, stabilita l'insussistenza di profili di violazione della disciplina di protezione dei dati personali in relazione alla designazione degli incaricati del trattamento e alle istruzioni ai medesimi impartite, come pure in relazione alla redazione del documento programmatico della sicurezza, è invece pervenuto a diverse conclusioni circa il rapporto intercorrente tra Poste italiane S.p.A. e distinti operatori ai quali vengono affidati taluni servizi di recapito della

corrispondenza, in virtù di contratti di appalto regolati da appositi "accordi quadro", aventi ad oggetto il *"servizio di distribuzione e raccolta di corrispondenza e posta non indirizzata ed espletamento dei servizi ausiliari"*. La qualificazione in termini di distinto e autonomo "titolare del trattamento" delle società appaltatrici non è risultata conforme agli artt. 4, comma 1, lett. *f*) e *g*), 28 e 29 del Codice, in considerazione dei poteri spettanti solo a Poste italiane S.p.A., in particolare, di assumere decisioni relative alle finalità del trattamento; impartire istruzioni e direttive vincolanti, svolgere funzioni di controllo rispetto all'operato delle società appaltatrici e degli incaricati delle stesse.

Il Garante ha pertanto prescritto a Poste italiane S.p.A. di designare le società appaltatrici "responsabili del trattamento" ai sensi degli artt. 4, comma 1, lett. *g*) e 29, commi 4 e 5, del Codice.

Altra fattispecie esaminata nel corso dell'anno ha riguardato taluni documenti trasmessi dall'Ufficio del giudice di pace di Roma, riguardanti un procedimento monitorio pendente tra il cessionario di un credito vantato da un'agenzia matrimoniale facente parte di una rete di soggetti operanti in *franchising* e il debitore ceduto (cliente dell'agenzia). Dagli atti pervenuti era emerso, in particolare, che l'agenzia aveva consegnato al cessionario una copia del contratto di mediazione a fini matrimoniali stipulato con la cliente - contenente dati personali anche sensibili dell'interessata (in particolare, il credo religioso) - per consentire il recupero in sede giudiziale del corrispettivo ancora dovuto per le prestazioni di mediazione matrimoniale ricevute.

Dalle risultanze istruttorie, tuttavia, è emerso che, in termini generali, la società affiliante svolgeva attività di controllo nei confronti delle agenzie affiliate.

Lo stesso modello di contratto di mediazione a fini matrimoniali, utilizzato da tutti i soggetti della rete menzionata statuiva che il cliente, all'atto del conferimento dell'incarico, desse il consenso al trattamento dei propri dati personali non solo all'agenzia con la quale veniva stipulato, ma anche all'affiliante ed alle altre agenzie della rete, e che i medesimi dati potessero essere oggetto di comunicazione nell'ambito dell'intera rete commerciale.

Infine, nello stesso contratto di affiliazione erano dettate specifiche norme per

l'eventuale risoluzione del rapporto di affiliazione commerciale e, in particolare, l'obbligo per l'affiliata di restituire la modulistica in giacenza, nonché tutti gli archivi e di cedere la gestione e la titolarità dei clienti in essere alla data di cessazione del contratto alla società affiliante o ad altri soggetti (incluse agenzie affiliate) dalla stessa indicati. Tale circostanza si era verificata nel caso di specie, come dimostrato dalla lettera di risoluzione contrattuale inviata dalla affiliante all'agenzia oggetto della segnalazione.

Il Garante ha pertanto ritenuto che, nel caso di specie, sia la società affiliante, sia le singole agenzie affiliate dovessero essere considerate quali *"contitolari del trattamento"* dei dati personali dei clienti (artt. 4, comma 1, lett. *f*) e 28 del Codice).

Inoltre, considerato che: mediante il modello di contratto di mediazione utilizzato da tutti i soggetti operanti nell'ambito della rete di agenzie matrimoniali venivano trattati anche dati sensibili dei clienti, tra cui, in particolare, quelli idonei a rivelarne le convinzioni religiose; i dati sensibili possono essere trattati da soggetti privati solo con il consenso scritto e informato degli interessati e sempre che il medesimo trattamento sia autorizzato preventivamente dal Garante, anche tramite autorizzazioni generali (artt. 26, 40 e 41 del Codice); il trattamento di dati sensibili da parte di agenzie matrimoniali è stato oggetto di *autorizzazione* generale n. 5/2009, capo V e VI [doc. *web* n. 1683005], il Garante ha ritenuto che, anche il trattamento dei dati idonei a rivelare le convinzioni religiose dei clienti effettuato nel perseguimento delle finalità connesse allo svolgimento dell'attività di mediazione a fini matrimoniali rientrasse nell'ambito di applicazione della menzionata autorizzazione generale.

Al contrario, la comunicazione di tali informazioni - come pure di altri dati sensibili riferiti agli interessati - è stata ritenuta sproporzionata ove effettuata in favore di soggetti preposti dalla società all'espletamento di attività aventi contenuto del tutto diverso (incluse le attività di recupero di crediti vantati verso i clienti).

Il Garante ha pertanto vietato (*Provv.* 4 febbraio 2010 [doc. *web* n. 1700869]) alla società l'ulteriore comunicazione dei dati sensibili riferiti ai clienti a soggetti preposti all'espletamento di specifici compiti non compatibili con il loro trattamento, anche con riguardo al recupero crediti, prescrivendo la riformulazione sia del modello di contratto

utilizzato per acquisire gli incarichi di mediazione matrimoniale da parte della clientela (in modo da prevedere l'inserimento dei dati sensibili dei clienti, inclusi quelli idonei a rivelare la confessione religiosa, in un'apposita sezione, da trasmettere solo se necessario), sia dell'informativa resa ai clienti (in termini compatibili con gli elementi di cui all'art. 13 del Codice).

10.7. TRATTAMENTO DI DATI E LIBRO SOCI

Un cittadino aveva lamentato il mancato riscontro alla richiesta - avanzata anche nel corso delle assemblee ordinarie, ai sensi dell'art. 2422 c.c, alla società di cui deteneva alcune azioni - di ispezionare il libro dei soci e di ottenere il rilascio di copia integrale del medesimo su supporto digitale senza l'oscuramento degli indirizzi dei soci-azionisti.

La richiesta era motivata dalla volontà di mettersi in contatto con gli altri soci al fine di tutelare i propri diritti e quelli dell'azionariato di minoranza (*cfr.* artt. 2367, 2408 e 2409 c.c.).

Al riguardo, l'Autorità ha precisato con *provvedimento* 26 marzo 2009 [doc. *web* n. 1606023] quanto già stabilito in precedenza in materia con *provvedimento* 19 dicembre 2000 [doc. *web* n. 1426274], affermando che la disciplina di protezione dei dati personali non contrasta con le disposizioni del codice civile relative alla documentazione e alla trasparenza dell'attività societaria, e segnatamente con la disciplina che prevede il diritto di ispezione del libro dei soci (art. 2422 c.c.). La comunicazione dei dati contenuti nel libro soci (anzitutto dei dati indicati all'art. 2421, comma 1, n. 1 del c.c.: *"il numero delle azioni, il cognome e il nome dei titolari delle azioni nominative, i trasferimenti e i vincoli ad esse relativi e i versamenti eseguiti"*), trattandosi di un obbligo previsto dalla legge (che ne fissa modalità e condizioni), può avvenire senza il consenso degli interessati (art. 24, comma 1, lett. *a*), del Codice).

Più in particolare, rispetto al dato relativo all'indirizzo dei soci (elemento che non compare nella previsione normativa *cit.*), dalla lettura complessiva della normativa di riferimento (*cfr.* art. 4 del r.d. 29 marzo 1942, n. 239 *"Norme interpretative, integrative e complementari del r.d.l. 25 ottobre 1941, n. 1148, convertito nella legge 9 febbraio 1942, n. 96,*

riguardante la nominatività obbligatoria dei titoli azionari" e art. 5, l. 29 dicembre 1962, n. 1745 "*Istituzione di una ritenuta d'acconto o di imposta sugli utili distribuiti dalle società e modificazioni della disciplina della nominatività obbligatoria dei titoli azionari*") è emerso che il libro dei soci ha un contenuto informativo più ampio rispetto alle indicazioni contenute nell'art. 2421 c.c., dovendo contenere, tra l'altro, il domicilio di ciascun socio.

Il Garante ha dunque fatto presente che anche tali informazioni devono essere comunicate, in occasione dell'esercizio del diritto di ispezione, al socio che eventualmente può ottenere anche estratti a proprie spese, senza il consenso degli interessati.

Così precisata l'estensione del diritto di ispezione previsto dall'art. 2422 c.c., il Garante ha comunque dichiarato inammissibile la richiesta dell'azionista di ordinare alla società di consentire l'ispezione al libro dei soci, dal momento che tale potere è comunque rimesso all'autorità giudiziaria ordinaria.

11. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Le operazioni di trasferimento dei dati personali all'estero sono state oggetto di particolare attenzione nel corso di tutto il 2009, sia con riferimento allo strumento delle *Binding corporate rules* (*Bcr*) (Norme vincolanti d'impresa), sia relativamente alla materia delle *Standard contractual clauses* (Clausole contrattuali tipo).

Il lavoro di approfondimento condotto dal Gruppo Art. 29, in relazione alle modalità e ai tempi di approvazione delle *Binding corporate rules*, ha prodotto positivi risultati in materia di accelerazione dei termini di definizione delle procedure di cooperazione europea e di proficua partecipazione delle autorità di protezione dei dati alla definizione dei testi da sottoporre ad autorizzazione nazionale. In più casi è stato interessato il Garante che, nel pronunciarsi favorevolmente in ordine ai progetti di *Bcr* elaborati da diversi gruppi societari di carattere multinazionale, si è dichiarato disponibile all'instaurazione della procedura nazionale volta al rilascio della relativa autorizzazione.

Molte delle procedure appena menzionate sono state condotte nell'ambito dell'accordo di mutua collaborazione assunto da 18 autorità (tra cui il Garante italiano) con l'obiettivo di accelerarne i tempi di conclusione e di semplificare l'attività di revisione degli schemi di *Bcr* predisposti dalle società.

Particolarmente intensa è stata, inoltre, l'attività di riflessione condotta in materia di *Standard contractual clauses* con riferimento alla proposta della Commissione europea volta all'adozione di un nuovo *set* di clausole da titolare a responsabile. In merito, diversi sono stati i contributi forniti da questa Autorità nell'ambito delle attività di approfondimento condotte dal Gruppo Art. 29 e relativamente alla redazione del parere in materia (*Opinion WP 161*).

Analoga attenzione è stata dedicata all'analisi della decisione della Commissione di recente approvazione (n. 2010/87/EU del 5 febbraio 2010) che, nel dar corso alla proposta succitata, sostituisce il *set* di clausole contrattuali tipo da titolare a responsabile, già esistente (decisione della Commissione n. 2002/16/EC), con un nuovo schema il quale, nel tentativo di meglio rappresentare la complessa realtà dell'affidamento

in *outsourcing*, prevede al proprio interno una clausola, *cd. "di subcontracting"* secondo la quale l'importatore (in qualità di responsabile del trattamento) può affidare il trattamento (o una parte di esso) a un soggetto terzo (*cd. "subcontractor"*), che agisce anch'esso come responsabile. E' tuttora in corso di definizione l'attuazione, con autorizzazione del Garante, della decisione medesima.

12. LIBERE PROFESSIONI

12.1. ORDINI PROFESSIONALI

Nel corso del 2009 l'Autorità ha fornito alcuni chiarimenti a professionisti circa le modalità con le quali gli ordini o i collegi professionali possono legittimamente trattare i dati personali dei propri iscritti.

In particolare, un ingegnere aveva ipotizzato una presunta violazione del Codice per la mancata pubblicazione, nell'albo, dei numeri di telefono, di fax e degli indirizzi di posta elettronica di alcuni colleghi. Dall'esame della normativa di settore è risultato che nell'albo degli ingegneri devono essere inseriti, per ogni singolo iscritto, il nome, il cognome e la residenza, che per i cittadini dell'Unione europea è parificata al domicilio professionale ai fini dell'iscrizione o del mantenimento in albi (*cfr.* art. 3, r.d. 23 ottobre 1925, n. 2537, art. 16, l. 21 dicembre 1999, n. 526).

Inoltre, il Codice prevede che gli ordini e collegi professionali possono, a richiesta della persona iscritta all'albo che vi abbia interesse, inserire nei rispettivi albi dati ulteriori rispetto a quelli previsti dalla normativa di settore, pertinenti e non eccedenti, in relazione all'attività professionale (*cfr.* art. 61, comma 3, del Codice).

Su tali basi l'Ufficio ha ritenuto che la mancata pubblicazione sull'albo degli ingegneri di informazioni ulteriori rispetto a quelle previste dalla normativa di settore non violasse il Codice (*Nota* 11 novembre 2009).

Il Consiglio nazionale del notariato (Cnn) aveva manifestato al Garante l'intenzione di realizzare un sistema centralizzato di archiviazione dei dati personali riportati nei repertori ed archivi degli studi notarili e di utilizzare tali dati, in forma anonima, per finalità statistiche, conferendo la gestione del sistema alla società che realizza e cura i servizi informatici e telematici per i notai italiani.

Per garantire il pieno rispetto della normativa, l'Autorità ha evidenziato che il predetto sistema di archiviazione può essere realizzato sempreché ogni singolo notaio, che decida di aderire all'iniziativa, designi la società Notartel quale responsabile del trattamento dei suddetti dati (art. 29 del Codice). È stata, inoltre, richiamata l'attenzione sul rispetto

degli obblighi di sicurezza e delle misure minime indicate nelle regole tecniche di cui all'Allegato B. al Codice (artt. 31, 33 *ss.* del Codice).

In merito al trattamento dei suddetti dati per finalità statistiche, l'Autorità ha evidenziato la necessità che presso il Cnn si proceda preventivamente alla costituzione dell'ufficio di statistica, nel rispetto del quadro normativo di settore, anche con riferimento all'informativa da rendere agli interessati (*cfr.* d.lgs. 6 settembre 1989, n. 322); infatti le informazioni in questione si qualificano come dati personali, ancorché non direttamente identificativi, a norma del Codice e del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (art. 4, comma 1, lett. *c*) e Allegato A.3. al Codice [doc. *web* n. 43293]) (*Nota* 21 ottobre 2009).

12.2. ATTIVITÀ FORENSE

Anche nel 2009 si è registrato un incremento dell'attività legata alle segnalazioni e ai reclami relativi all'attività forense, con particolare riferimento al trattamento di dati personali anche sensibili effettuato dagli avvocati nell'ambito di procedimenti giudiziari civili e penali.

Produzione di documenti in giudizio

In merito alla produzione di documenti di varia natura in sede giudiziaria, l'Autorità ha ribadito che ogni valutazione in ordine alla validità, efficacia e utilizzabilità in giudizio di atti, documenti e provvedimenti basati sul trattamento di dati personali, anche ove il trattamento medesimo non sia conforme alle disposizioni di legge o di regolamento, spetta, ai sensi dell'art. 160, comma 6, del Codice, al giudice e non al Garante (*Note* 27 ottobre 2009, 5 novembre 2009 e 16 ottobre 2009).

Visione e copia di atti processuali

Nel caso di presa visione ed estrazione di copia di atti contenuti nei fascicoli processuali, l'Autorità ha ricordato che il Codice (art. 51) non ha modificato le norme concernenti la visione ed il rilascio di estratti e di copie di atti e documenti, contenute nei codici di procedura civile e penale (*Nota* 22 ottobre 2009).

Il consenso degli interessati

Alcune segnalazioni hanno riguardato il trattamento di dati personali in sede giudiziaria da parte di avvocati senza il consenso degli interessati. In tali occasioni l'Autorità ha

rappresentato che, ai sensi dell'art. 24, comma 1, lett. *f*), del Codice, il consenso non è richiesto quando il trattamento è necessario *"per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento"*. Ha inoltre precisato che, in tali ipotesi, non è richiesta l'informativa all'interessato, ove i suoi dati personali siano raccolti presso terzi (art. 13, comma 5, lett. *b*), del Codice) (*Note* 16 ottobre 2009, 5 novembre 2009 e 20 ottobre 2009).

Conservazione dei dati

E' stato affrontato il tema dei limiti temporali della conservazione, da parte degli avvocati, di dati personali, anche sensibili, successivamente alla conclusione del processo al quale afferiscono.

A tale proposito, il Garante ha ricordato (*Nota* 5 novembre 2009) che il codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria ([doc. *web* n. 1565171], *v. Relazione 2008*, p. 166) stabilisce, al riguardo (art. 4), che la definizione di un grado di giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati da parte del difensore.

Una volta estinto il procedimento o il relativo rapporto di mandato, atti e documenti attinenti all'oggetto della difesa o delle investigazioni difensive possono essere conservati, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento.

Con specifico riferimento ai dati sensibili, inoltre, l'Autorità ha ricordato (*Nota* 5 novembre 2009) che l'*autorizzazione* n. 4/2008 al trattamento dei dati sensibili da parte dei liberi professionisti [doc. *web* n. 1529408] prevede al punto 5) che i dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

Alcune segnalazioni hanno riguardato anche il trattamento dei dati personali svolto da investigatori privati.

In particolare, in un caso è stata posta la questione del mandato a svolgere attività investigative in sede di indagini preliminari rilasciata, ad un investigatore privato, dalla parte

personalmente, benché l'art. 327-*bis* c.p.p., in tema di attività investigative svolte nel corso di indagini preliminari, preveda, al comma 3, che tali attività possano essere svolte da investigatori privati autorizzati su incarico del difensore.

Nell'occasione l'Autorità ha osservato (*Nota* 27 ottobre 2009) che - ferma ogni eventuale conseguenza sul piano processuale che non spetta al Garante valutare, e con esclusivo riferimento agli aspetti riguardanti la protezione dei dati personali - il codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive, nel disciplinare anche i trattamenti da parte di investigatori privati, stabilisce che questi possono svolgere le loro attività solo sulla base di uno specifico mandato scritto, che può essere rilasciato sia da un legale, sia da altro soggetto (art. 8, commi 2 e 6).

A seguito di alcune segnalazioni, l'Autorità ha, inoltre, accertato il rispetto del menzionato codice deontologico da parte di alcune agenzie investigative, con particolare riferimento al rispetto degli obblighi di non divulgare a terzi le informazioni raccolte e dell'effettiva consegna ai committenti, al termine delle indagini, di tutta la documentazione raccolta (*Nota* 9 febbraio 2010).

13. TRATTAMENTO DEI DATI PERSONALI IN AMBITO CONDOMINIALE

Alcuni condòmini avevano lamentato l'illecita affissione in spazi accessibili al pubblico, da parte dell'amministratore del condominio, di un avviso di rimozione delle loro autovetture parcheggiate nel cortile condominiale (oggetto di lavori per la costruzione di posti auto interrati), indicante il numero di posto auto, le targhe dei veicoli, nonché le foto delle auto medesime. Gli stessi segnalanti avevano inoltre contestato l'indebita comunicazione a terzi (il legale di fiducia dello stesso condominio e soggetti incaricati, a vario titolo, dei lavori) dell'inosservanza di una delibera assembleare e della targa della relativa autovettura.

L'Autorità (*Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]) rilevato che, nel caso di specie, si sarebbero potute adottare modalità parimenti efficaci ma meno invasive per gli interessati, ha ritenuto la predetta affissione contraria ai princìpi di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), prescrivendo al condominio di rivolgersi singolarmente ai partecipanti alla compagine condominiale. Parimenti illecita e sproporzionata è risultata la comunicazione ai soggetti a vario titolo coinvolti nell'appalto dei dati personali riferiti agli interessati; ciò tenuto conto che la mancata rimozione degli autoveicoli riconducibili ai segnalanti risultava già comprovata dal materiale fotografico prodotto in atti e che la presenza *in loco* delle stesse imprese appaltatrici (impossibilitate all'esecuzione dei lavori deliberati proprio in ragione della presenza dei veicoli non rimossi) non giustifica tale comunicazione.

È stata dunque vietata al condominio l'ulteriore comunicazione ai soggetti sopra menzionati dei dati riferiti ai segnalanti, ma è stata ritenuta lecita la comunicazione dei predetti dati al legale, considerata la necessità manifestata dal condominio di doversi tutelare in sede giudiziaria (art. 24, comma 1, lett. *f*), del Codice).

Il Garante si è occupato (anche) delle modalità di presentazione della denuncia relativa al calcolo e al versamento della tassa per lo smaltimento dei rifiuti solidi urbani (*cd.* "Tarsu").

In particolare, il *provvedimento* 19 febbraio 2009 [doc. *web* n. 1601650]

ha ad oggetto la comunicazione dei dati personali riferiti ad un condòmino da parte dell'amministratore, nell'ambito della procedura di trasmissione al comune competente, dei dati utili al calcolo della tassa menzionata.

Il conduttore di un immobile, con reclamo, aveva lamentato il deposito, da parte dell'amministratore del condominio, della denuncia di *"occupazione o detenzione di locali o aree"* ai fini del versamento della Tarsu, relativa alla sua posizione tributaria. Benché avesse già assolto tale obbligo di denuncia e diffidato l'amministratore dal provvedervi, per effetto della dichiarazione inoltrata, a sua insaputa, dall'amministratore stesso, il reclamante avrebbe ricevuto la notifica di due avvisi di pagamento riferiti allo stesso periodo di occupazione per il medesimo immobile.

Il regolamento comunale, in assenza della trasmissione dei dati da parte dei soggetti tenuti alla dichiarazione, per tali posizioni residue poneva in capo agli enti proprietari, agli enti gestori o agli amministratori di condominio la responsabilità del versamento di quanto dovuto (art. 27, comma 3, regolamento *cit.*).

Con il citato *provvedimento* il Garante, nel ritenere il trattamento lecito in astratto (art. 24, comma 1, lett. *a*), del Codice) ha tuttavia ritenuto che la comunicazione nei confronti degli uffici comunali fosse avvenuta in violazione del principio di correttezza (art. 11, comma 1, lett. *a*), del Codice).

Infatti l'amministratore, per evitare la consegna di dichiarazioni diverse riferite allo stesso contribuente e al contempo prevenire l'insorgere di una possibile responsabilità a proprio carico avrebbe dovuto, prima della comunicazione dei dati del reclamante, accertarsi presso gli uffici comunali competenti dell'effettivo mancato adempimento dell'obbligo gravante sul soggetto passivo della tassa.

Pertanto l'Autorità ha prescritto, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, all'amministratore condominiale di porre in essere ogni previa scrupolosa verifica dell'avvenuta presentazione della stessa da parte degli occupanti dello stabile amministrato al fine di prevenire denunce ripetute o inesatte.

14. SICUREZZA DEI DATI E DEI SISTEMI

14.1. CONSERVAZIONE DEI DATI DI TRAFFICO: MISURE E ACCORGIMENTI A GARANZIA DEI CITTADINI

Anche nel 2009, il Garante si è occupato di questioni legate al tema della conservazione dei dati di traffico telefonico e telematico sia per finalità di accertamento e repressione dei reati sia per altre finalità ordinarie.

In primo luogo, il Garante è nuovamente intervenuto in relazione ai termini entro i quali i fornitori di servizi telefonici e telematici sono tenuti a conformare i propri sistemi alle misure e agli accorgimenti prescritti con il *provvedimento* 17 gennaio 2008 [doc. *web* n. 1482111] come integrato il 24 luglio 2008 [doc. *web* n. 1538224], dei quali si è dato atto nella *Relazione 2008*, p. 173.

Infatti, nel mese di aprile 2009 numerose richieste di associazioni rappresentative del settore delle comunicazioni elettroniche hanno rappresentato una situazione di sostanziale, ma non ancora integrale, adeguamento, per la quasi totalità dei fornitori, alle prescrizioni contenute nel suindicato provvedimento, con particolare riferimento alle misure e agli accorgimenti prescritti alla lettera *a*), nn. 3, 6 e 9 e alla lettera *c*) dello stesso.

Le medesime associazioni hanno, quindi, richiesto al Garante una proroga dei termini indicati nel citato *provvedimento* del 24 luglio 2008, al fine di completare l'attuazione delle richiamate prescrizioni, rispetto alle quali peraltro i fornitori hanno dichiarato di aver già raggiunto un elevato livello di adeguamento.

L'Autorità in ragione dell'elevato numero di piattaforme e sistemi aziendali coinvolti negli adempimenti previsti dal provvedimento, dell'altrettanto elevato numero di processi aziendali da essi supportati e, quindi, della complessità degli interventi necessari per l'adeguamento degli stessi, nonché della mole degli investimenti complessivi previsti e di quelli già impegnati ha accordato la richiesta proroga, anche se limitatamente ad alcune misure specificamente indicate. Pertanto, con il *provvedimento* 29 aprile 2009 (in *G.U.* 11 maggio 2009, n. 107 [doc. *web* n. 1612508]), è stato individuato il nuovo termine nel 15 dicembre 2009, prevedendo altresì che, entro la medesima data, tutti i titolari del

trattamento interessati dovessero dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento.

Nel corso dell'anno, inoltre, l'Autorità ha svolto una verifica sul rispetto della normativa in materia di *data retention* da parte dei fornitori di servizi telefonici e telematici che operano in Italia.

La menzionata attività va ricondotta anche alla decisione del Gruppo Art. 29 di disporre un'azione di *enforcement* volta a verificare l'osservanza, da parte dei fornitori di servizi di comunicazione elettronica, degli obblighi fissati nella normativa nazionale in materia di *data retention*, sul fondamento degli artt. 6 e 9 della Direttiva n. 2002/58/CE e della Direttiva n. 2006/24/CE.

La complessa attività istruttoria ha riguardato servizi telefonici e telematici - individuati, in primo luogo, tra quelli che non erano stati oggetto degli accertamenti svolti dall'Autorità sin dal 2005 e dei provvedimenti adottati nel corso dell'anno 2008 - sulla base di alcuni criteri ai quali aveva fatto riferimento anche il Gruppo Art. 29 (*ad es.*, il fatto di essere operatori telefonici "virtuali" ovvero fornitori di servizi esclusivamente telematici).

In particolare, è stato consegnato ai quattro fornitori coinvolti nell'accertamento, unitamente a richieste di informazioni ai sensi dell'art. 157 del Codice sull'attuazione degli adempimenti sopra indicati, un questionario appositamente predisposto nell'ambito dell'*enforcement.*

In base alle risposte pervenute, l'Autorità ha proceduto nei mesi di settembre e ottobre con gli accertamenti ispettivi presso le sedi delle società, concentrandosi essenzialmente sulle criticità emerse rispetto alla disciplina della *data retention*, risultate peraltro, nella maggior parte dei casi, di facile risoluzione tecnica.

L'Autorità in ragione delle violazioni accertate - tempi di conservazione dei dati di traffico telefonico e telematico superiori al consentito; conservazione di informazioni sui siti visitati dagli utenti - ha successivamente adottato tre *provvedimenti* (21 ottobre 2009 [doc. *web* n. 1683093] e 19 novembre 2009 [doc. *web* nn. 1695393 e 1695368]) nei confronti di altrettante società tra quelle coinvolte nell'istruttoria, disponendo in due casi

anche la trasmissione degli atti alla magistratura per la valutazione di eventuali profili penali.

Al riguardo l'Autorità ha innanzitutto prescritto la cancellazione dei dati di traffico telefonico e telematico conservati oltre i tempi previsti dalla normativa a fini di accertamento e repressione dei reati (12 mesi per i dati di traffico telematico e 24 mesi per quelli di traffico telefonico).

Ha inoltre prescritto di cancellare tutte le informazioni in grado di rivelare gusti, opinioni, tendenze degli utenti che non avrebbero mai dovuto essere archiviate nei *database* (*ad es.*, l'oggetto dei messaggi di posta elettronica inviati e ricevuti; i dati personali relativi alla navigazione in internet, anche quando rappresentati dal solo indirizzo *Ip* di destinazione).

Ad una società è stato prescritto, al fine di innalzare i livelli di sicurezza dei flussi informativi con l'autorità giudiziaria e di garantire in modo più adeguato la riservatezza delle informazioni, di sostituire il fax con sistemi di comunicazione sviluppati con protocolli di rete sicuri e strumenti di cifratura basati su firma digitale.

14.2. IL RUOLO DEGLI AMMINISTRATORI DI SISTEMA NELLA SICUREZZA DEI TRATTAMENTI

Come indicato nella *Relazione 2008* (p. 178 *ss.*), il ruolo dell'amministratore di sistema e la rilevanza strategica di questa figura nell'ambito della protezione dati sono stati oggetto di interesse da parte dell'Autorità che, con *provvedimento* 27 novembre 2008 (*G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]), aveva richiamato tutti i titolari di trattamenti effettuati, anche solo in parte, mediante strumenti elettronici, alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, individuando altresì le misure da adottare per agevolare la verifica sull'attività degli amministratori da parte dei titolari delle banche dati e dei sistemi informatici.

In ragione della complessità degli interventi organizzativi e tecnici a tali fini necessari e delle richieste pervenute da numerosi soggetti pubblici e privati, il Garante ha

successivamente avviato una consultazione pubblica (*Provv.* 21 aprile 2009, in *G.U.* 8 maggio 2009, n. 105 [doc. *web* n. 1611986]) volta ad acquisire osservazioni ed opinioni tecniche da parte dei titolari del trattamento ai quali il provvedimento originale era rivolto. La consultazione, durata poco più di un mese, ha coinvolto numerosi soggetti pubblici, le principali aziende del settore dell'*information technology*, nonché alcune importanti associazioni di categoria, mettendo in luce la complessità tecnica di attuazione del provvedimento riscontrata in alcune realtà pubbliche e private di grandi dimensioni.

La consultazione ha inoltre ha fatto emergere importanti considerazioni relative ai trattamenti effettuati mediante l'uso di servizi in *outsourcing* e di terze parti in qualità di amministratori di sistema.

Pertanto, in ragione dei contributi pervenuti e delle considerazioni maturate nell'ambito della consultazione pubblica, l'Autorità ha differito al 15 dicembre 2009 i termini di adeguamento al provvedimento (*Provv.* 25 giugno 2009, in *G.U.* 30 giugno 2009, n. 149 [doc. *web* n. 1626595]), introducendo anche alcune modifiche al testo originale, per semplificare l'implementazione delle misure previste nei casi di trattamenti effettuati in *outsourcing* o mediante subappalti della gestione dei sistemi informativi.

15. LA VIDEOSORVEGLIANZA E LA BIOMETRIA

15.1. VIDEOSORVEGLIANZA IN AMBITO PUBBLICO

L'attività nel periodo considerato ha riguardato l'applicazione del *provvedimento* generale in materia di videosorveglianza del 2004 ([doc. *web* n. 1003482], *cfr. Relazione 2004*) e, in seguito a consultazioni di carattere istituzionale con l'Anci (Associazione nazionale comuni italiani) ed il Ministero dell'interno, l'adozione del nuovo *provvedimento* in materia (8 aprile 2010 [doc. *web* n. 1712680]).

Per quanto riguarda il *provvedimento* del 2004 l'Autorità, nel rispondere a molteplici segnalazioni e quesiti, ha fornito ulteriori indicazioni sulla sua corretta applicazione.

Numerosi comuni hanno adottato uno specifico regolamento disciplinante le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio, che hanno successivamente trasmesso al Garante per ottenerne l'approvazione ovvero solo per porre a conoscenza l'Autorità di tale iniziative. Al riguardo, è stato rappresentato che l'installazione di tali sistemi non deve essere sottoposta all'esame preventivo dell'Autorità. In particolare, non può desumersi alcuna approvazione implicita dal silenzio del Garante dopo la ricezione di regolamenti, progetti o comunicazioni relativi all'intenzione di installare tali sistemi (*cfr.* punto 3.2., *Provv. cit.*) (*Note* 13 novembre 2009, 20 novembre 2009 e 13 gennaio 2010).

Ad uno dei comuni che aveva trasmesso il proprio regolamento l'Ufficio ha, altresì, precisato che le iniziative di videosorveglianza devono essere precedute da una corretta valutazione, alla luce dei princìpi di liceità, necessità, pertinenza, non eccedenza e proporzionalità rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice). Pertanto, non risulta lecito procedere ad una videosorveglianza capillare di intere aree cittadine "cablate", riprese integralmente, costantemente e senza adeguate esigenze (*cfr.* punto 5.1., *Provv. cit.*) (*Nota* 20 luglio 2009).

Un comune aveva manifestato l'intenzione di montare stabilmente telecamere, per sole riprese video, a bordo di veicoli utilizzati dalla polizia locale, ma privi di contrassegni identificativi dell'ente di appartenenza, con la finalità specifica di contrastare il fenomeno

dell'abbandono dei rifiuti sul territorio di competenza. Al riguardo, è stato precisato che non sono previste, da parte del Garante, ipotesi di autorizzazione per esentare dall'obbligo di fornire l'informativa agli interessati nell'ambito di un trattamento di dati personali effettuato tramite sistemi di videosorveglianza (art. 13 del Codice). Nel citato *provvedimento* è specificato che coloro i quali transitano nelle aree sorvegliate devono essere informati della rilevazione dei dati. L'informativa deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi (*cfr.* punto 3.1. *Provv. cit.*) (*Nota* 13 gennaio 2010).

Si è fatto più volte presente che resta, tuttavia, ferma l'esenzione, prevista dalla legge, dall'obbligo di fornire l'informativa agli interessati in relazione alle ipotesi di trattamento di dati personali effettuato *"da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento e repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento"* (art. 53 del Codice) (*Note* 9 dicembre 2009 e 13 gennaio 2010).

Infine, l'Autorità è stata chiamata, in più occasioni, a pronunciarsi sui tempi di conservazione delle immagini raccolte tramite sistemi di videosorveglianza.

In particolare, Sogei S.p.A. (società di *information and communication technology* del Ministero dell'economia e delle finanze), che gestisce i dati, anche sensibili, di tutti i contribuenti e di tanti altri cittadini, aveva chiesto di essere autorizzata a conservare le immagini raccolte oltre le ventiquattro ore, così come previsto dal *provvedimento* del 2004 (*cfr.* punto 3.4., *Provv. cit.*), e per un periodo massimo di sette giorni. Con riferimento ai tempi di conservazione, il Garante ha stabilito che va comunque applicato il principio di proporzionalità e che, quindi, l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere le finalità perseguite (art. 11, comma 1, lett. *d*) ed *e*) del Codice).

In tale quadro, vista la particolare rischiosità dell'attività che svolge la Sogei per la natura dei dati trattati, l'Ufficio ha ritenuto proporzionato che la stessa conservi le immagini raccolte tramite sistemi di videosorveglianza per un periodo di tempo non superiore alla settimana (*Nota* 11 novembre 2009).

L'Autorità si è espressa nei medesimi termini nei confronti della Soprintendenza per i beni storici, artistici e etnoantropologici per le province di Bo, Fe, Fc, Ra, e Rn, che aveva chiesto, per le immagini raccolte presso la Pinacoteca Nazionale di Bologna, la conservazione per un tempo superiore alle ventiquattro ore e non eccedente le settimana (*Nota* 10 febbraio 2010).

Da ultimo, si menziona la vicenda relativa alla Soprintendenza speciale per il polo museale napoletano che si era rivolta all'Autorità dopo aver ricevuto dal Comando dei Carabinieri-tutela patrimonio culturale nucleo di Napoli la richiesta di conservare le immagini raccolte tramite i sistemi di videosorveglianza, installati presso alcuni siti museali della Regione Campania, per un periodo di almeno trenta giorni, al fine di tutelare, nell'ambito del progetto *"Allarme sicurezza musei"*, i siti d'interesse culturale che potrebbero essere maggiormente esposti al rischio della minaccia terroristica. Dall'esame della normativa di settore è emerso che è possibile effettuare controlli continuativi tramite impianti audiovisivi per garantire la sicurezza dei beni culturali raccolti nei musei statali (art. 1, d.l. 14 novembre 1992, n. 433).

Il Garante ha precisato che, anche nelle ipotesi in cui specifiche disposizioni di legge consentano l'installazione di telecamere in tema di sicurezza, è comunque necessario - qualora siano trattati dati relativi a persone identificate o identificabili - rispettare i princìpi generali di liceità, necessità, proporzionalità e finalità affermati dal Codice (artt. 3, 11, comma 1, lett. *a*) e *d*) e 18, comma 2, del Codice e punto 2.1., *Provv. cit.*).

Inoltre, ha ribadito che, in base al principio di proporzionalità, l'eventuale allungamento, oltre una settimana, dei tempi di conservazione di tali dati deve essere valutato come eccezionale e relativo a specifiche necessità derivanti da eventi già accaduti o realmente incombenti, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso (*cfr.* punto 3.4., *Provv. cit.*). Alla luce delle considerazioni sopra richiamate, il Garante ha prescritto alla Soprintendenza speciale per il polo museale napoletano, con *provvedimento* adottato ai sensi dell'articolo 154, comma 1, lett. *c*) del Codice, di conservare le immagini raccolte presso alcuni siti museali della Regione Campania

per un periodo di trenta giorni, finché persiste la dichiarata eccezionale necessità (*Provv.* 12 marzo 2009 [doc. *web n.* 1605521]).

In ordine ai sistemi di videosorveglianza, è da rilevare l'approvazione (condizionata) di un apparato di videosorveglianza presso un istituto scolastico di Verona, sottoposto a verifica preliminare dell'Autorità, nell'ambito di un progetto più ampio denominato *"Scuole sicure"*, a fini di prevenzione e deterrenza contro teppismo ed atti vandalici, a salvaguardia del patrimonio scolastico.

Il Garante ha approvato tale progetto, con taluni limiti, a tutela di ragazzi, docenti e personale scolastico. E' stata disposta infatti, in conformità al *provvedimento* generale sulla videosorveglianza del 29 aprile 2004, l'entrata in funzione delle telecamere solo negli orari di chiusura degli istituti; in caso di attività all'interno della scuola che potrebbero iniziare e concludersi in coincidenza con l'orario di attivazione delle telecamere è stata prevista l'esigenza di definire, in accordo con il dirigente scolastico, gli orari di funzionamento delle telecamere.

Le telecamere possono riprendere esclusivamente le mura esterne, devono essere segnalate da appositi cartelli con visibilità anche notturna e la visualizzazione delle immagini è stata consentita solo a polizia e autorità giudiziaria (*Provv.* 4 settembre 2009 [doc. *web* n. 1651744]).

Il nuovo provvedimento in materia di videosorveglianza

Il nuovo *provvedimento* generale in materia di videosorveglianza [doc. *web* n. 1712680], che sostituisce quello del 29 aprile 2004 [doc. *web* n. 1003482], adottato visto lo sviluppo della tecnologia, i numerosi interventi normativi, statali e regionali - che hanno incentivato l'utilizzo della videosorveglianza come forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici, nonché le molteplici finalità per le quali tali sistemi sono utilizzati - delinea un nuovo quadro di garanzie a tutela degli interessati fornendo, contestualmente, specifiche prescrizioni ai titolari del trattamento.

In considerazione della rilevanza della tematica, se ne dà conto di seguito in dettaglio.

Preliminarmente sono stati consultati il Ministero dell'interno, l'Associazione nazionale comuni italiani (Anci) e l'Unione delle province d'Italia (Upi), affinché ciascuno, per i propri profili di competenza, formulasse le proprie osservazioni.

In base al provvedimento, in primo luogo, in conformità ai princìpi di necessità e proporzionalità, vanno preferiti, se possibile, dati anonimi e, comunque, raccolte solo immagini pertinenti e non eccedenti rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *d*), del Codice).

Gli interessati devono essere resi edotti dell'esistenza di sistemi di videosorveglianza. Al tal fine, si può utilizzare lo stesso modello semplificato di informativa "minima" messo a disposizione nel *provvedimento* del 2004 (art. 13, comma 3, del Codice). Inoltre, il supporto con l'informativa deve essere chiaramente visibile anche quando il sistema di videosorveglianza sia, eventualmente, attivo in orario notturno. È stato, altresì, predisposto un nuovo modello semplificato di informativa "minima" per i titolari del trattamento che intendono attivare un collegamento diretto con le forze di polizia.

E' tuttavia auspicabile, in particolare, che l'informativa semplificata rinvii ad un testo completo, contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente e senza oneri per gli interessati.

Inoltre è stato prescritto che l'impiego di sistemi di raccolta delle immagini associate a dati biometrici e dei sistemi *cd. "intelligenti"* - capaci, cioè, di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli - sia sottoposto alla verifica preliminare, trattandosi di attività di videosorveglianza che comporta rischi specifici per i diritti e le libertà fondamentali.

Per quanto riguarda le misure di sicurezza (artt. 30, 33 *ss.* e Allegato B. al Codice), l'Autorità ha disposto, in particolare, che: agli incaricati e responsabili del trattamento siano conferiti diversi livelli di visibilità e trattamento delle immagini, in relazione alle diverse competenze di ciascuno; siano limitate le ipotesi di visione delle immagini raccolte e registrate; siano predisposte specifiche misure per la cancellazione delle immagini conservate, anche tramite sistemi di sovra-registrazione; sia del tutto eccezionale l'accesso alle immagini nelle ipotesi di manutenzione del sistema; vengano disposti sistemi di protezione da accessi abusivi per gli apparati di ripresa digitali; siano applicate tecniche crittografiche nelle ipotesi di trasmissione di immagini da una rete pubblica o tramite connessioni *wireless*.

Fatte salve speciali esigenze di ulteriore conservazione in relazione alla chiusura di uffici o esercizi, o a specifica richiesta investigativa delle autorità preposte, le immagini devono essere conservate al massimo per ventiquattro ore, dopo la loro rilevazione. La cancellazione può avvenire anche tramite meccanismi automatici di rimozione dei dati obsoleti e gestione automatica delle *policy di retention.* E' ammesso un più ampio tempo di conservazione dei dati, non oltre la settimana, solo in alcuni casi correlati a peculiari esigenze tecniche o alla particolare rischiosità dell'attività svolta dal titolare del trattamento.

Per i comuni e nelle sole ipotesi in cui la videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*, per le quali, ferma restando l'eccezionalità dell'ipotesi, occorre richiedere una verifica preliminare del Garante.

Merita menzione la decisione dell'Autorità di ritenere lecita l'attività di videosorveglianza al fine sia di accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose, sia di monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, sempreché tali finalità non possano essere perseguite senza ricorrere al trattamento di dati personali.

La videosorveglianza può essere effettuata da soggetti pubblici, nel rispetto del principio di finalità, per lo svolgimento delle proprie funzioni istituzionali e fornendo previamente idonea informativa agli interessati, anche nei casi in cui i sindaci, quali ufficiali del Governo, ed i comuni utilizzano sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

La rilevazione di immagini tramite sistemi di videosorveglianza svolta da soggetti privati può avere legittimamente luogo previa acquisizione del consenso degli interessati o in presenza di un requisito equipollente (artt. 23 e 24 del Codice). A tal proposito, il *provvedimento* ha individuato i casi in cui - al fine di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di

vandalismo, o per finalità di prevenzione di incendi o di sicurezza del lavoro - la rilevazione di immagini da parte di soggetti privati può avvenire senza previa acquisizione del consenso degli interessati.

Il Garante ha affrontato anche il tema della videosorveglianza nei condomìni, evidenziando che è stata inoltrata una segnalazione al Governo e al Parlamento volta a sollecitare la disciplina di problemi applicativi emersi negli ultimi anni, concernenti, in particolare, la competenza e le modalità di delibera dell'assemblea condominiale ai fini dell'istallazione degli impianti di videosorveglianza.

Con riferimento ai *cd. "sistemi integrati di videosorveglianza"* tra diversi soggetti, sia pubblici che privati, sono state previste specifiche garanzie relative ai trattamenti di dati effettuati mediante: la gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; il collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; il collegamento con le forze di polizia, anche nelle predette ipotesi.

Al riguardo, sono state prescritte alcune misure di sicurezza ulteriori concernenti, in particolare: l'adozione di sistemi per la registrazione degli accessi logici effettuati e delle operazioni compiute sulle immagini registrate; la separazione logica delle immagini registrate dai diversi titolari.

Con specifico riferimento ai sistemi di videosorveglianza integrati utilizzati dagli enti territoriali, inoltre, non possono essere tracciati gli spostamenti degli interessati e le immagini gestite da un unico centro devono essere trattate in forma differenziata.

Devono essere sottoposti a verifica preliminare i sistemi integrati di videosorveglianza non rientranti nei modelli sopra descritti e per i quali non sia possibile adottare le misure e gli accorgimenti indicati nel provvedimento.

In considerazione del fatto che anche i dispositivi elettronici per la rilevazione di violazioni al codice della strada comportano un trattamento di dati personali, nel circoscrivere le ipotesi di rilevazione di immagini in caso di infrazione, sono stati disciplinati il regime di accessibilità ed i relativi tempi di conservazione prevedendo, altresì, specifiche

cautele per la riservatezza di eventuali passeggeri presenti a bordo dei veicoli.

In tale ambito è stato precisato che, quando il codice della strada prevede espressamente che si renda nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni o quando il titolare del trattamento utilizza comunque i modelli predisposti in conformità al medesimo codice della strada, è possibile fare a meno di fornire un'ulteriore distinta informativa.

Sono stati infine indicati specifici termini - il cui mancato rispetto può comportare l'applicazione di una sanzione amministrativa - entro i quali i titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza sono tenuti ad adeguarsi alle prescrizioni o ad adempiere agli obblighi richiamati nel provvedimento, successivamente pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

15.2. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Muovendo dalle risultanze di un accertamento ispettivo disposto d'ufficio, l'Autorità ha valutato la liceità del trattamento svolto per il tramite di un impianto di videosorveglianza installato presso un ipermercato (*Provv.* 26 febbraio 2009 [doc. *web* n. 1601522]). Il sistema, alla luce degli elementi acquisiti, è risultato installato anche in aree dell'ipermercato suscettibili di transito da parte dei lavoratori (*box* informazioni; *caveau*; zona di scarico merci), senza che tuttavia fosse stata rispettata la disciplina che regola i controlli a distanza dell'attività dei lavoratori (art. 4, comma 2, della legge 20 maggio 1970, n. 300, *cd.* "statuto dei lavoratori").

Le risultanze documentali hanno altresì evidenziato l'assenza di cartelli recanti l'informativa da rendere agli interessati, nonché la conservazione delle immagini registrate per un arco temporale non giustificato da motivate esigenze organizzative.

Inoltre, i dipendenti che avevano accesso alle immagini, benché ritualmente designati quali incaricati in relazione ad altre tipologie di trattamento, non lo sono risultati relativamente allo specifico trattamento svolto per il tramite del sistema di videosorveglianza installato.

Alla luce di tali considerazioni, l'Autorità ha ritenuto illecito il trattamento perché

in violazione degli artt. 11, comma 1, lett. *a*) ed *e*), e 114, del Codice, disponendone conseguentemente, nelle more dell'eventuale espletamento delle procedure sindacali previste dal richiamato art. 4 dello statuto dei lavoratori, il blocco (limitatamente al trattamento svolto presso le aree suscettibili di transito da parte dei lavoratori), prescrivendo altresì al titolare l'adozione di alcune specifiche misure e accorgimenti a tutela degli interessati (con particolare riferimento all'informativa, ai tempi di conservazione delle immagini e alla specifica designazione dei soggetti incaricati alla loro visione quali incaricati del trattamento).

Sull'installazione di un sistema di videosorveglianza all'interno di un complesso condominiale (*Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]) si è riferito nel *par.* 13.

Di altri casi, nei quali l'utilizzo di sistemi di videosorveglianza si univa al trattamento di dati biometrici, si riferisce di seguito.

15.3. BIOMETRIA

In considerazione della frammentaria regolamentazione della materia è stato attivato un gruppo di lavoro per approfondire diversi profili dell'utilizzo di dati biometrici a fini di sicurezza e per scopi diversi (scopi facilitativi). Il gruppo, composto da professori universitari, rappresentanti del DigitPA (già Cnipa) ed esperti della materia, ha il compito di fornire indicazioni utili al riesame della disciplina in materia, con riferimento all'ambito di applicazione della verifica preliminare e della notificazione del trattamento. A tal fine il gruppo ha preso in considerazione i sistemi e le modalità di trattamento di dati biometrici maggiormente utilizzati, in particolare l'impiego di dati biometrici a fini di verifica/identificazione, per procedere ad una loro classificazione in base al reale grado di rischiosità per i diritti e le libertà degli interessati.

Gli interventi dell'Autorità nel corso dell'anno sono stati diretti, in primo luogo, ad assicurare il rispetto dei princìpi di necessità e proporzionalità nell'utilizzo dei dati biometrici.

Biometria e luoghi di lavoro

Con specifico riferimento al trattamento di dati biometrici sul posto di lavoro, il Garante si è pronunciato sull'impiego di un sistema di rilevazione di impronte digitali

dei dipendenti da parte di una concessionaria di automobili (*Provv.* 15 ottobre 2009 [doc. *web* n. 1664257]), che aveva inizialmente dichiarato di voler utilizzare il sistema per verificare la presenza in servizio. A seguito delle indicazioni fornite dall'Ufficio (che richiamava al rispetto delle *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"* [doc. *web* n. 1364939]), la concessionaria aveva rappresentato di voler comunque continuare nell'impiego del sistema, sia pure per il perseguimento di finalità diverse da quelle originariamente comunicate. Il rilevatore biometrico sarebbe stato utilizzato per consentire l'accesso all'area "officina" - ritenuta sensibile per la presenza in loco di apparecchiature asseritamente pericolose e di beni di valore (parti di ricambio di autoveicoli) - e solo in via residuale, eventualmente, per verificare l'effettiva presenza dei lavoratori sul luogo di lavoro.

Gli accertamenti ispettivi espletati *in loco* hanno evidenziato l'esistenza di un sistema biometrico idoneo alla rilevazione delle presenze dei lavoratori e alla commisurazione delle ore lavorative dagli stessi prestate. Attraverso un apposito *software* collegato al sistema, infatti, l'ufficio del personale è risultato in grado di formare il *"cartellino mensile delle presenze"* per ciascun dipendente e di visualizzare le relative "timbrature" aggiornate in tempo reale.

L'Autorità, nel confermare l'orientamento già espresso in passato (*Provv.* 21 luglio 2005 [doc. *web* n. 1150679]; *Provv.* 15 giugno 2006 [doc. *web* nn. 1306523, 1306530 e 1306551]; *Provv.* 2 ottobre 2008 [doc. *web* n. 1571502]), ha ritenuto illecito il trattamento, in quanto effettuato dalla concessionaria in assenza di legittimi presupposti (non risultando dalla documentazione specifiche giustificazioni per l'utilizzo di tali peculiari modalità di trattamento) e in violazione dei princìpi di necessità e proporzionalità; ciò a cagione del fatto che il controllo dei lavoratori autorizzati ad entrare nell'area officina avrebbe potuto essere agevolmente effettuato (stante anche l'esiguità del numero dei dipendenti interessati) ricorrendo a modalità alternative (*ad es.*, tramite *badge*); inoltre, la sperimentalità del sistema avrebbe potuto essere ugualmente verificata senza il coinvolgimento dei lavoratori (*ad es.*, tramite gli stessi installatori, ovvero disabilitando

la funzionalità di registrazione delle fasce orarie dei dipendenti). Peraltro, l'illiceità del trattamento svolto è derivata anche dall'inosservanza, da parte della concessionaria, delle garanzie procedurali previste dall'art. 4 della legge 20 maggio 1970, n. 300, così come interpretato dalla recente giurisprudenza proprio in riferimento alle apparecchiature in grado di controllare il rispetto degli orari di entrata e uscita e la presenza sul luogo di lavoro dei dipendenti (Cass. 17 luglio 2007, n. 15892). L'Autorità ha dunque vietato alla concessionaria l'ulteriore trattamento dei dati biometrici dei dipendenti per finalità di rilevazione delle loro presenze e di commisurazione dei relativi tempi di lavoro.

Il Garante è poi intervenuto nei confronti di un importante centro orafo campano adottando, all'esito di una complessa attività istruttoria, un *provvedimento* di divieto e prescrizioni in materia di trattamento di dati personali sia mediante l'impiego di un impianto di videosorveglianza, sia mediante l'installazione di un sistema di rilevazione di dati biometrici.

Il centro, che riunisce quasi quattrocento imprese operanti nel settore dei preziosi, era stato sottoposto a una ispezione per verificare l'uso dei sistemi di videosorveglianza. Gli accertamenti del Garante avevano evidenziato che la società che lo gestisce non aveva predisposto né un'informativa adeguata, né cartelli idonei a segnalare ai lavoratori e ai visitatori la presenza delle circa centoquaranta telecamere installate per monitorare tutta l'area. Era risultata, peraltro, la conservazione delle immagini per un tempo superiore a quello indicato dal Garante con il *provvedimento* generale in materia di videosorveglianza del 29 aprile 2004 [doc. *web* n. 1003482].

Con *provvedimento* del 4 giugno 2009 [doc. *web* n. 1629975], il Garante ha pertanto prescritto alla società di fornire l'informativa agli interessati, nelle forme (semplificate) previste dal modello allegato al *provvedimento* del 2004, con riguardo a tutte le aree interessate dal sistema di videosorveglianza installato a presidio del centro orafo, nonché di integrare tali informazioni, per le aree diverse da quelle esterne, con avvisi circostanziati (riportanti gli elementi di cui all'art. 13 del Codice) collocati presso i varchi d'accesso al centro orafo; ha prescritto altresì di conservare le immagini in relazione alle effettive necessità della raccolta, e comunque, in ragione dell'area geografica ad alto tasso di

criminalità nella quale è stabilito il centro orafo e della natura dei beni ivi commercializzati, per non oltre una settimana.

Con il medesimo provvedimento l'Autorità ha vietato l'uso, in forma centralizzata, dei dati biometrici (*template* tratti dalle impronte digitali) raccolti mediante un sistema di rilevamento utilizzato al fine di agevolare l'accesso al centro orafo di soci ed operatori del settore accreditati. La società, infatti, non aveva addotto ragioni specifiche volte a chiarire la necessità della memorizzazione in un sistema centralizzato dei menzionati *template* e, pertanto, tale misura è stata considerata sproporzionata, ben potendosi adottare - in conformità ai princìpi stabiliti negli artt. 3 e 11, comma 1, lett. *d*), del Codice - misure meno invasive a tutela degli interessati (quali, *ad es.*, sistemi biometrici nei quali il *template* ricavato dalle impronte digitali risiede su una *smart card* posta nell'esclusiva disponibilità del detentore o basati sulla lettura del contorno della mano: in questo senso *v.* l'esito della verifica preliminare condotta su un caso analogo nel *Provv.* 1° febbraio 2007 [doc. *web* n. 1381983]).

Ulteriori contestazioni avevano riguardato la modulistica utilizzata per raccogliere il consenso al trattamento dei dati personali di quanti accedevano all'area. Agli interessati, infatti, veniva sottoposto un unico modulo che autorizzava la società a usare i dati biometrici per l'accesso e i dati personali anagrafici per finalità di *marketing*. Alla società è stato perciò prescritto sia di predisporre nuovi modelli di raccolta del consenso, tali da permettere una libera e autonoma scelta da parte dell'interessato sull'uso dei propri dati, sia di integrare l'informativa fornita nella modulistica con gli elementi mancanti (art. 13 del Codice).

La società ha, successivamente, comunicato di essersi conformata alle prescrizioni del Garante.

Sulle medesime tematiche il Garante è tornato a pronunciarsi nei confronti di un'altra società, che eroga il servizio di trasporto pubblico su gomma nell'ambito di un comune campano e di alcune località limitrofe.

In primo luogo, in relazione al trattamento di dati personali effettuato tramite un sistema di videosorveglianza installato presso un deposito di stazionamento degli autobus,

il periodo di conservazione dei dati registrati era risultato superiore a quanto previsto con il *cit.* provvedimento generale del 2004 e, pertanto, non conforme all'art. 11, comma 1, lett. *e*), del Codice.

Con *provvedimento* del 29 ottobre 2009 [doc. *web* n. 1682066] il Garante ha pertanto prescritto di conservare le immagini in relazione alle effettive necessità della raccolta, nei termini previsti dal menzionato provvedimento generale.

In ordine, poi, ai trattamenti effettuati mediante un sistema di rilevazione di dati biometrici basato sulla elaborazione di *template* tratti dalla lettura delle impronte digitali dei lavoratori operanti alle dipendenze della società, considerato che, in sede ispettiva, non erano risultate comprovate specifiche esigenze idonee a giustificare l'utilizzo di dati biometrici, né per la natura delle attività ivi svolte né, in particolare, per verificare il puntuale adempimento della prestazione lavorativa, il Garante ha disposto nei confronti della società (nelle more della definizione di un procedimento di verifica preliminare medio tempore attivato con apposito interpello), il blocco del trattamento dei dati biometrici dei lavoratori, già trattati illecitamente per accertarne la presenza sul luogo di lavoro, con conseguente possibilità di procedere alla sola conservazione temporanea dei medesimi dati.

La società ha, successivamente, comunicato di essersi conformata alle prescrizioni del Garante.

Relativamente alla sicurezza negli aeroporti il Garante (*Provv.* 17 settembre 2009 [doc. *web* n. 1655708]), in sede di verifica preliminare (art. 17 del Codice), ha autorizzato una società che svolge attività di vigilanza e sicurezza a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa.

Nel progetto sottoposto alla verifica era previsto che i dati biometrici dei dipendenti, costituiti da caratteristiche tratte dall'impronta digitale, fossero memorizzati sotto forma di *template* ed in modalità cifrata, su un supporto (*smart card*) posto nell'esclusiva disponibilità del lavoratore. Il progetto escludeva comunque il controllo sull'orario di lavoro.

L'Autorità ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei

dipendenti in relazione agli accessi alle sole *"aree sterili"*. Ha tuttavia prescritto alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa sulla natura facoltativa del consenso al trattamento dei dati biometrici. La conservazione dei dati relativi agli accessi alle *"aree sterili"* è stata approvata per un tempo massimo di sette giorni.

Analogamente, l'uso di dati personali biometrici per l'accesso ad aree riservate, è stato ammesso dal Garante anche per i locali in cui sono custodite banche di dati personali di particolare rilevanza.

In dettaglio, una società concessionaria dei servizi relativi alle entrate e al recupero dell'evasione fiscale e tributaria per conto del Comune di Roma aveva manifestato al Garante l'esigenza di assicurare la riservatezza di una gran quantità di informazioni, anche di carattere sensibile.

Per evitare accessi indebiti alle aree che ospitano gli archivi informatici, la società aveva, quindi, richiesto la verifica preliminare in merito all'attivazione di un sistema di riconoscimento biometrico basato sull'impronta digitale dei dipendenti, memorizzata - sotto forma di *template* e cifrata - su una *smart card* priva di indicazioni nominative, affidata all'esclusiva disponibilità del lavoratore.

L'Autorità (*Provv.* 8 aprile 2009 [doc. *web* n. 1610018]) ha ritenuto proporzionato, per gli scopi suddetti, l'impiego di dati tratti dalle impronte digitali in ragione delle modalità previste, della delicatezza dei dati custoditi e del numero circoscritto di dipendenti interessati dal sistema di rilevazione.

16. IL REGISTRO DEI TRATTAMENTI

L'art. 154, comma 1, lett. *l*), del Codice impone all'Autorità di tenere il *"registro dei trattamenti"*, formato sulla base delle notificazioni ricevute ai sensi degli artt. 37 e 38. In particolare, l'art. 37, comma 4, stabilisce che il Registro sia accessibile a chiunque e che la sua consultazione gratuita avvenga per via telematica attraverso il sito *web* dell'Autorità.

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.

Per quanto concerne più specificamente il contenuto della notificazione, occorre ricordare che sin dal 2004 l'Autorità aveva posto in essere profondi cambiamenti in relazione alla relativa procedura, e che ulteriori snellimenti delle modalità di compilazione del modello informatico e dei suoi contenuti sono stati disposti con la modifica dell'art. 38, nel quadro delle finalità di semplificazione e accelerazione delle procedure amministrative previste dall'art. 29 del d.l. n. 112/2008, come modificato dalla legge di conversione n. 133/2008.

Il nuovo modello di notificazione, introdotto con *provvedimento* del Garante del 22 ottobre 2008, oltre ad una generale riorganizzazione del modello stesso, ha tra l'altro 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.

E' rimasto inalterato l'ormai tradizionale servizio di assistenza *online*, realizzato con messaggi di posta elettronica (tanto originati in automatico dalla procedura quanto predisposti in modo specifico dal personale addetto), sempre affiancato dal supporto telefonico. Anche nel 2009 questi servizi hanno registrato un positivo *trend* di crescita, quantitativa e qualitativa. I meccanismi di controllo in tempo reale della procedura sono stati ulteriormente affinati, garantendo una ancor più rapida ed efficiente risposta ai problemi dell'utenza. Le difficoltà riscontrate sono peraltro ridotte in maniera sensibile, tanto per i miglioramenti intervenuti nella procedura che per la maggiore confidenza

del pubblico con gli strumenti utilizzati (pagamenti *online*, firma digitale, consultazione telematica).

E' aumentato il numero dei cittadini interessati al contenuto del Registro che si sono avvalsi del servizio di ausilio offerto dal Dipartimento. Sono altresì numerosi gli accessi diretti al Registro da parte degli utenti, con una media giornaliera che ha superato i novanta accessi, e punte superiori ai trecento. Tale modalità di fruizione delle notificazioni è segno della effettiva realizzazione del dettato dell'art. 37, comma 4, del Codice, sulla consultazione telematica gratuita del Registro. In tal senso, si sono rivelate decisive le funzioni di stampa integrale delle notificazioni (un tempo da richiedere al Dipartimento), la possibilità di seguire l'*iter* delle diverse modifiche e cessazione successive alla prima notificazione anche in caso di modifica totale della denominazione del titolare, le modalità di ricerca, semplice ma realmente efficace.

Sono ovviamente proseguite le attività di controllo delle notificazioni effettuate e di accertamento delle violazioni dell'obbligo di notificazione, in vista delle attività ispettive del Garante.

Il 2009 ha fatto registrare una inversione di tendenza rispetto al numero delle notificazioni presentate, con una contrazione di circa il 15% rispetto all'anno precedente.

Risultano stabili, dopo la forte contrazione dell'anno scorso, le notificazioni di trattamenti relativi a dati idonei a rivelare lo stato di salute e la vita sessuale, mentre si consolida il numero dei trattamenti di dati effettuati con strumenti elettronici e volti a definire il profilo o la personalità dell'interessato, o ad analizzarne abitudini o scelte di consumo.

Per quanto concerne la distribuzione geografica dei titolari, si conferma il distacco del nord del Paese (nord est e nord ovest rappresentano ormai il 56% dei titolari presenti) rispetto al resto del territorio; ciò oltre che a diversità economiche di natura strutturale, potrebbe esser da collegare anche ad elementi legati alla fase più acuta della crisi economica, che ha maggiormente inciso sulla tipologia di titolari presenti nel sud (ditte individuali, artigiani, società a responsabilità limitata di piccole o piccolissime dimensioni).

17. LA TRATTAZIONE DEI RICORSI

17.1. CONSIDERAZIONI GENERALI

La prima osservazione sull'attività istruttoria e decisoria svolta nell'anno 2009 in relazione ai ricorsi proposti ai sensi degli artt. 145 *ss.* del Codice - che per la trasversalità e l'eterogeneità dei temi affrontati, si presta maggiormente a riflessioni di carattere generale - è la constatazione di un rinnovato, significativo aumento delle trattazioni.

Dopo diversi anni (dal 2005 in avanti) che avevano visto un progressivo calo nel numero di decisioni assunte, l'anno appena trascorso segna (dopo l'assestamento già registratosi nel 2008) un aumento apprezzabile delle decisioni adottate (il totale dell'anno ammonta a trecentosessanta).

Lo strumento del ricorso appare, quindi, sempre vitale. Per un verso si consolida come strumento ordinario e consueto per consentire il "dominio" dell'interessato sui dati personali che lo riguardano (attraverso l'esercizio del diritto di accesso) o per ripristinare il controllo sulle informazioni illegittimamente trattate (a mezzo delle richieste di blocco, cancellazione od opposizione al trattamento). Per altro verso è uno strumento duttile che si adatta efficacemente agli ambiti e alle situazioni più diverse e consente agli interessati (spesso impegnati o protesi verso contenziosi di più ampia portata) di disporre di potenzialità nuove per sostenere le proprie ragioni e interloquire efficacemente nella dialettica processuale. Ne sono prova i tanti procedimenti che dimostrano come i diritti tutelati dall'art. 7 del Codice hanno una imprevedibile e amplissima possibilità di adattarsi ai contesti più diversi, spesso aprendo scenari nuovi e "costringendo" l'Autorità a confrontarsi continuamente e innovativamente con le categorie generali disciplinate dalla legge e dalla direttiva comunitaria.

E' in realtà il concetto base di "dato personale" che ha una oggettiva, ampia possibilità di espansione e soprattutto di adattamento ai nuovi contesti tecnologici con i quali quotidianamente l'Autorità si deve confrontare. In effetti, un esame più approfondito dei tanti casi affrontati mette in luce come la presenza e le potenzialità della rete internet sia sempre più lo sfondo delle decisioni sui ricorsi.

Vengono in considerazione non solamente il fenomeno dello *spamming* a fini genericamente promozionali e pubblicitari, ma soprattutto le conseguenze dell'utilizzo della rete - specie quelle di lungo periodo indotte dalla persistenza sulla rete stessa dei dati - che sono emerse negli ultimi mesi. La diffusione, senza limiti di durata, delle informazioni e la loro facile reperibilità su internet grazie all'ausilio dei *cd.* "motori di ricerca", se da un lato espande e facilita le possibilità conoscitive, dall'altro (specie in caso di informazioni inesatte, incomplete o addirittura lesive della dignità della persona) aumenta i rischi di danno legati appunto ad una loro persistenza indefinita, capace di porre nel nulla le aspettative connesse al *cd.* "diritto all'oblìo".

Questi temi, già difficili da affrontare in relazione al comune funzionamento della rete, diventano di ancora più complessa soluzione, utilizzando gli ordinari strumenti giuridici, con riferimento al fenomeno in prepotente e velocissima espansione dei *cd. "social network"*. In tale ambito, determinare le fattispecie eventualmente sottoponibili al campo di applicazione della legge è operazione assai complessa.

Se le sfide delle nuove tecnologie si sono affacciate anche nella trattazione di diversi ricorsi, bisogna comunque osservare che, anche nel 2009, lo "zoccolo duro" degli ambiti trattati si conferma ancora quello più "tradizionale" emerso negli ultimi anni.

Ancora una volta è l'insieme dei trattamenti di dati ruotanti attorno alla realtà bancaria e finanziaria ad assorbire il maggior numero di trattazioni, includendo in questo totale i numerosi casi di esame della disciplina concernente la Centrale rischi della Banca d'Italia, l'archivio della *cd.* "centrale d'allarme interbancaria", i trattamenti concernenti i sistemi di informazioni creditizie.

Merita poi di essere evidenziato il significativo aumento delle trattazioni concernenti il trattamento dei dati dei dipendenti (sia da parte di datori di lavoro pubblici che privati) nonché quelle riferite ai trattamenti svolti in ambito giornalistico (nell'ampia accezione in cui il termine è considerato dal Codice).

Infine, un'ultima notazione sul tipo di decisioni adottate riguarda l'elevatissimo numero di declaratorie di "non luogo a provvedere".

Ciò conferma che, spesso, dopo l'iniziale silenzio serbato dai titolari del trattamento

a fronte degli interpelli proposti dagli interessati, la presentazione formale del ricorso al Garante apre la strada ad una rapida definizione della vicenda, superando ostacoli e ritardi spesso determinati da incompleta o inesatta conoscenza delle disposizioni del Codice.

17.2. PROFILI PROCEDURALI

La vasta casistica affrontata nel corso dell'anno consente di estrarre diverse decisioni che consentono di far emergere aspetti significativi connessi alla procedura dei ricorsi. Ciò, mettendo in luce sia aspetti ormai consolidati nella "giurisprudenza" del Garante, sia problematiche nuove oggetto di primo esame da parte dell'Autorità.

Si propongono di seguito alcuni casi di particolare interesse.

17.2.1. Proponibilità del ricorso nei confronti di particolari soggetti

Il ricorso, come detto, è strumento di amplissimo utilizzo. Pur tuttavia, esistono ambiti particolari nei quali, per espressa disposizione del Codice, tale strumento di tutela non trova applicazione o situazioni nelle quali emerge l'errata individuazione di un soggetto quale (supposto) titolare di un determinato trattamento.

A tal proposito, si può citare la *decisione* del 3 novembre 2009 [doc. *web* n. 1687662] con la quale è stato rilevato il difetto di legittimazione passiva di *Google Italy S.r.l.* in ordine al rinvenimento, per il tramite del noto motore di ricerca *"Google"*, di una pagina *web* contenente informazioni ritenute inesatte dalla ricorrente. L'istruttoria svolta ha messo in luce l'estraneità della società evocata nel procedimento (*Google Italy S.r.l.*) rispetto al trattamento di dati in questione, limitandosi la predetta società ad una *"mera attività di* marketing, *ricerca clienti e raccolta della pubblicità"*.

Particolarmente interessante è anche la vicenda culminata nella *decisione* del 16 luglio 2009 [doc. *web* n. 1638472] con la quale è stato dichiarato inammissibile un ricorso proposto nei confronti dell'amministrazione del Senato della Repubblica in relazione ai dati personali di una persona citata nel testo di un'interrogazione parlamentare risalente nel tempo e tuttora disponibile sul sito internet del Senato.

Nel caso di specie il Garante ha anzitutto rilevato le esigenze di tutela e i problemi connessi alla prolungata reperibilità sulla rete di informazioni suscettibili di riverberarsi in negativo sulla figura e l'identità dell'interessato. Ma l'Autorità ha altresì riscontrato che lo specifico trattamento in questione viene effettuato nell'esercizio di funzioni e prerogative parlamentari e in ossequio al principio relativo alla pubblicità degli atti parlamentari. Tale trattamento, svolto appunto da un organo costituzionale, è disciplinato dallo stesso in conformità al rispettivo ordinamento nell'ambito della sfera di autonomia riservata alle Camere dalla Costituzione (art. 64 Cost.). Ciò induce a ritenere che la legge sulla protezione dei dati non possa regolare tale ambito riservato di spettanza parlamentare, in ragione della *"indipendenza guarentigiata"* delle Camere nei confronti di ogni altro potere, riconosciuta anche dalla Corte costituzionale (sentenza n. 154 del 1985).

Va poi ricordata l'ulteriore *decisione* 4 febbraio 2010 [doc. *web* n. 1703923] che ha sancito l'inammissibilità di un ricorso proposto nei confronti dell'Agenzia informazioni e sicurezza esterna (Aise), trattandosi di soggetto - al pari di tutti gli altri organismi di informazione e sicurezza - nei cui confronti non può essere attivata la procedura dei ricorsi (ai sensi dell'art. 58 del Codice).

17.2.2. Tempistica e formalità per la proposizione dei ricorsi

Il procedimento dei ricorsi, anche in ragione dei previsti termini assai brevi, è caratterizzato da requisiti formali minimi e da una notevole agilità procedurale. Tuttavia alcuni punti fermi sono stati più volte ribaditi dall'Autorità al fine di evitare che la doverosa attenzione al dato sostanziale non determini incertezza e indeterminazione nelle modalità di esercizio dei diritti. Va in questa direzione il *provvedimento* 22 dicembre 2009 [doc. *web* n. 1695163] che - nel ricordare che in termini generali il ricorso può essere proposto solo dopo che siano trascorsi quindici giorni dall'avvenuta ricezione, da parte del titolare del trattamento, dell'interpello preventivo - ha rammentato l'esigenza di una prova della sussistenza del presupposto (ovvero un *"pregiudizio imminente e irreparabile"*) che solo può giustificare la presentazione immediata del ricorso, senza seguire appunto il procedimento ordinario che richiede la previa proposizione di un'istanza ai sensi dell'art. 7 del Codice.

Va vista in quest'ottica anche la *decisione* del 12 giugno 2009 [doc. *web* n. 1633383] che ha ribadito la perentorietà del termine (sette giorni dalla richiesta in tal senso fatta pervenire dall'Ufficio del Garante) per l'eventuale regolarizzazione dei ricorsi, ferma restando la possibilità di attivare un nuovo procedimento al riguardo nel rispetto delle forme e dei termini di cui agli artt. 145 *ss.* del Codice.

17.2.3. Trattamenti per fini esclusivamente personali

Il sensibile aumento della casistica ha messo in rilievo nel corso dell'anno l'importanza della disposizione di cui all'art. 5, comma 3, del Codice secondo cui il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si tratta di una "norma-filtro" volta a limitare l'ambito di applicazione del Codice di cui l'Autorità ha recentemente fatto uso in diverse ipotesi. Basti citare i *provvedimenti* del 12 giugno 2009 [doc. *web* n. 1634343] e del 23 luglio 2009 [doc. *web* n. 1639978] nei quali l'Autorità non ha ritenuto applicabile la normativa del Codice a trattamenti effettuali da persone fisiche per fini esclusivamente personali e in assenza di sistematica comunicazione o di diffusione.

Non meno significative (e strettamente legate al nuovo contesto tecnologico) sono le *decisioni* del 12 giugno 2009 [doc. *web* n. 1633575] e del 22 dicembre 2009 [doc. *web* n. 1695177]. Con esse l'Autorità si è confrontata con la necessità di definire, in riferimento alla citata disposizione di cui all'art. 5, comma 3, il concetto di *"comunicazione sistematica"*, che non è stato riconosciuto nelle due fattispecie, ricondotte appunto all'ipotesi del trattamento per fini esclusivamente personali. Nella prima vicenda era stato contestato l'invio di un consistente numero di e-mail ad una *mailing list* di magistrati amministrativi in relazione a una complessa vicenda concorsuale che aveva visto partecipi entrambe le parti del ricorso e che aveva altresì suscitato l'interesse di alcune testate giornalistiche. Alla luce della documentazione prodotta dalle parti, la delineata comunicazione è risultata essere stata effettuata dal resistente nella veste di persona fisica che, in quanto oggetto di una segnalazione disciplinare e successivamente autore di un ricorso presentato dinanzi

al Tar per l'annullamento di un concorso pubblico al quale lo stesso aveva partecipato, ha rappresentato *"ad una cerchia ben delineata (seppur ampia) di destinatari (tutti i magistrati amministrativi), i propri convincimenti e le proprie iniziative in merito a tale vicenda"*. Ciò tenendo conto che la comunicazione in oggetto (consistente nell'invio di informazioni e documenti relativi al ricorrente) risultava essere stata effettuata una volta sola e rivolta nei confronti di soggetti che il resistente, a vario titolo, riteneva possibili interventori nel citato giudizio innanzi al Tar.

Nel secondo caso si è fatta applicazione dei medesimi princìpi in un ricorso rivolto nei confronti di un moderatore di una *mailing list* che aveva comunicato un'informazione errata relativa al ricorrente. Anche in questo caso l'inammissibilità del ricorso è derivata dall'applicazione dell'art. 5, comma 3, del Codice, atteso che la *mailing list* in questione era relativa a un *"gruppo chiuso"*, con la conseguenza che i messaggi postati non erano disponibili per i soggetti allo stesso non appartenenti.

17.2.4. Particolari ambiti di esercizio del diritto di accesso

La già evidenziata ampiezza del concetto di dato personale determina una correlata gamma di ambiti nei quali vengono proposte istanze di accesso ai sensi del Codice, determinando con ciò la creazione di veri e propri "filoni" spesso funzionali alla gestione di specifici contenziosi. Ne è sicuro esempio il rilevante numero di casi che, richiamando il disposto dell'art. 9, comma 3, del Codice, si incentrano sulla richiesta di accedere a dati personali di defunti. Ciò, in particolare, con riguardo alla ricostruzione delle posizioni bancarie intestate al *de cuius*, al fine di determinare con esattezza l'ammontare dei cespiti ereditari. Ne sono esempio, fra le tante, la *decisione* del 12 novembre 2009 [doc. *web* n. 1688199], dove l'Autorità ha affrontato un caso di concorso fra successione testamentaria e successione legittima, e quella del 22 dicembre 2009 [doc. *web* n. 1695325] nella quale ha riconosciuto in capo ad un legatario *"l'interesse proprio"* di cui alla citata disposizione dell'art. 9.

Altro ambito delicato è quello sanitario dove l'esercizio del diritto di accesso è spesso finalizzato all'acquisizione di documentazione utile al fine di verificare, ed eventualmente

contestare, i trattamenti sanitari fruiti. Merita in proposito di essere ricordata la *decisione* del 17 settembre 2009 [doc. *web* n. 1656642] concernente la richiesta di accedere (da parte del convivente superstite) alle informazioni contenute nella cartella clinica e nei referti diagnostici della *de cuius* detenuti dalla struttura ospedaliera nella quale la stessa era stata ricoverata e dove successivamente era deceduta. Anche in questo caso la richiesta è stata accolta, atteso che il ricorrente, legato alla paziente defunta da un documentato rapporto di convivenza, ha esercitato il diritto al fine di disporre delle informazioni necessarie a intraprendere le azioni giudiziarie più opportune per la verifica di eventuali inadempienze nelle prestazioni sanitarie rese dalla resistente.

Ambito più tradizionale è invece quello connesso alle richieste di accesso ai dati personali trattati in ambito assicurativo, con particolare riguardo alle informazioni contenute nelle perizie medico-legali. Si tratta di profili su cui vi è una lunga serie di pronunciamenti dell'Autorità, già in relazione alle disposizioni della l. n. 675/1996. Ma il tema, per la sua rilevanza e la frequenza delle situazioni nelle quali si ripropone, continua a costituire materia di esame e di decisione in sede di ricorsi (*Provv.* 4 giugno [doc. *web* n. 1630066] e 17 settembre 2009 [doc. *web* nn. 1656632 e 1656621]). Ciò, con particolare riguardo alla concreta individuazione delle situazioni nelle quali possa essere invocato il differimento dell'esercizio del diritto di accesso in ragione della necessità di salvaguardare lo svolgimento delle investigazioni difensive o per tutelare l'esercizio del diritto in sede giudiziaria (art. 8, comma 2, lett. *e*), del Codice).

17.2.5. Modalità di riscontro

La pluralità di ambiti interessati dall'esercizio del diritto di accesso e la varietà di "tipologie" di dati (informazioni cartacee, dati trattati in formato elettronico, immagini, suoni, *ecc.*) propongono naturalmente problemi connessi alle modalità di messa a disposizione dei dati stessi. Sul punto può essere ricordata la *decisione* dell'8 gennaio 2010 [doc. *web* n. 1699486], correlata a una richiesta di acquisizione di dati originariamente trattati nell'ambito di una trasmissione televisiva, risultati poi disponibili sul sito internet dell'emittente televisiva.

Le modalità di riscontro sono, in termini generali, enunciate dall'art. 10 del Codice, ma al riguardo l'Autorità, con la predetta decisione, ha avuto modo di precisare che il titolare del trattamento può scegliere direttamente le modalità per fornire il riscontro (e, tra esse, anche quelle consistenti nella trasmissione delle informazioni per via telematica), salva la facoltà dell'interessato di pretendere che l'adempimento avvenga attraverso la trasposizione dei dati su uno specifico supporto in grado di agevolarlo in ragione dei mezzi tecnologici a propria disposizione e delle personali capacità di utilizzazione. Il Garante ha in proposito ulteriormente precisato che nel concetto di trasmissione dei dati deve farsi rientrare anche la diretta messa a disposizione, da parte del titolare, dei dati che riguardano l'interessato all'interno di un sito internet liberamente accessibile dal medesimo, purché le informazioni siano facilmente consultabili e risultino duplicabili senza dover necessariamente ricorrere a strumenti tecnologici particolarmente complessi. Sempre in relazione alle modalità di riscontro merita, infine, di essere ricordata la *decisione* dell'8 luglio 2009 [doc. *web* n.1638561] con la quale è stato riconosciuto il diritto dell'interessato di ottenere la comunicazione dei dati che lo riguardano relativi alla registrazione di un colloquio telefonico (*cd. "verbal ordering"*) con la società fornitrice del servizio telefonico attraverso, appunto, la messa a disposizione su apposito supporto della registrazione vocale originale della telefonata (strumento indispensabile per verificare, nel caso di specie, la reale conclusione di un accordo tra le parti).

17.3. AMBITI TEMATICI SIGNIFICATIVI

Già nel *par.* 17.1. si sono messi in evidenza i principali settori in ordine ai quali sono stati proposti i ricorsi *ex* art. 145 del Codice. In questa parte si esamineranno esclusivamente le problematiche connesse ai *cd. "archivi storici* online*"* e i principali ricorsi proposti in riferimento all'attività giornalistica.

17.3.1. Archivi storici online *e richiesta di cancellazione dei dati*

Si è rivelato uno degli ambiti più "vivaci" in ragione della quantità, diffusività e potenziale lesività dei dati trattati. Il fenomeno è già stato oggetto di attenzione nella

relazione dello scorso anno in riferimento ai primi casi venuti all'attenzione dell'Autorità (*cfr. Relazione 2008*, p. 200). Il tema è quello connesso all'integrale pubblicazione e diffusione sulla rete internet degli archivi storici dei principali quotidiani. Tale pubblicazione consente l'accesso ad un'enorme quantità di informazioni che vengono messe a disposizione del pubblico attraverso una modalità di consultazione estremamente agevole, facilitata oltretutto dalle possibilità offerte dai *cd.* "motori di ricerca". Ciò, però, può comportare la reperibilità di informazioni anche molto datate, spesso negativamente caratterizzate, che vengono in questo modo riattualizzate e accostate a persone che, nel frattempo, hanno intrapreso percorsi di vita lontani dalle situazioni e dal contesto cui la notizia faceva originariamente riferimento.

Si determina così un complesso intreccio e spesso un evidente conflitto tra diritti e valori egualmente meritevoli di tutela (il diritto alla riservatezza, la libertà di manifestazione del pensiero, il diritto alla libera ricerca storica, il diritto allo studio e all'informazione).

Rispetto a tale conflitto, che si specifica nelle richieste - che i ricorrenti avanzano - di cancellazione delle informazioni (contenute negli articoli a suo tempo pubblicati in forma cartacea) dai siti internet dei quotidiani, il Garante si è sforzato di individuare un punto di equilibrio.

Prima di tutto si è sottolineato come il trattamento dei dati personali dei ricorrenti sia in origine di per sé (generalmente) lecito per finalità giornalistiche, nel rispetto del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

La riproposizione dei medesimi dati nell'articolo pubblicato quale parte integrante dell'archivio storico del quotidiano rientra invece tra i trattamenti effettuati per concretizzare e favorire la libera manifestazione del pensiero e, in particolare, la libertà di ricerca, cronaca e critica anche storica.

In questo quadro, tale trattamento può essere effettuato senza il consenso degli interessati, è compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati e può essere effettuato, in termini generali, anche oltre il periodo di tempo necessario per conseguire tali diversi scopi (art. 99 del Codice). Di conseguenza, la

riproposizione *online* sul sito internet di un editore, di un articolo a suo tempo pubblicato sull'edizione cartacea, non dà luogo a un trattamento illecito di dati e non giustifica la rimozione dello stesso e la cancellazione dei relativi dati.

Il Garante ha però in diversi casi separatamente e favorevolmente considerato i motivi legittimi di opposizione connessi alle richieste di diversi interessati i quali hanno rappresentato legittimamente la propria aspirazione affinché in rete, per mezzo delle "scansioni" operate automaticamente dai motori di ricerca esterni al sito degli editori, non restassero associate perennemente ai propri nominativi notizie pubblicate molti anni prima. Il risultato è stato ottenuto prescrivendo agli editori (naturalmente nei soli casi di accoglimento di tali istanze) di "sottrarre", con appositi accorgimenti tecnici, la pagina *web* contenente i dati dell'interessato dalla diretta individuabilità tramite i più utilizzati motori di ricerca esterni, pur restando la medesima pagina inalterata nel contesto dell'archivio consultabile telematicamente accedendo in via diretta all'indirizzo *web* dell'editore interessato. Naturalmente questa tutela, per risultare equilibrata e non incidere sulle esigenze di una informazione che deve essere la più ampia possibile, deve tenere conto di elementi specifici e rilevanti quali il tempo trascorso dalla pubblicazione originaria della notizia, la notorietà o meno del soggetto che richiede tale particolare forma di tutela, il rilievo che la notizia può ancora riverberare in un determinato ambito.

Si tratta ovviamente di criteri che sono stati prudentemente elaborati sulla base della casistica sottoposta all'Autorità in questa prima fase di confronto con tale nuova problematica. Ne sono testimonianza, fra le altre, le *decisioni* del 25 giugno 2009 [doc. *web* n. 1635966] e del 23 luglio 2009 [doc. *web* n. 1639172] nelle quali le posizioni degli interessati sono state appunto salvaguardate attraverso la cennata sottrazione dei dati che li riguardavano, contenuti in notizie molto risalenti nel tempo, dalla scansione dei motori di ricerca esterni.

L'applicazione dei criteri sopra citati ha portato invece a due declaratorie di infondatezza con le *decisioni* del 22 maggio 2009 [doc. *web* n. 1635938] e del 28 maggio 2009 [doc. *web* n. 1635910]. In entrambi i casi le richieste di cancellazione di articoli relativi a pregresse vicende giudiziarie degli interessati non sono state accolte (neanche

in riferimento all'esclusione dell'indicizzazione degli articoli stessi dai motori di ricerca). Ciò in ragione del rilievo pubblico dei protagonisti e della notorietà politica (a livello nazionale in un caso, e locale in un altro) degli stessi. Tali elementi, uniti al fatto che le vicende sulle quali era incentrata la cronaca giornalistica erano state oggetto di attenzione e di sviluppi giudiziari anche in tempi più recenti, giustificano e rendono anzi opportuna, agli occhi del Garante, una ampia conoscibilità di tali informazioni anche attraverso un loro agevole reperimento sulla rete internet.

17.3.2. Trattamenti in ambito giornalistico - L'applicazione delle disposizioni normative e deontologiche

Come accennato in premessa, lo strumento del ricorso è frequentemente utilizzato per contestare la legittimità del trattamento di dati e informazioni in ambito giornalistico. L'impressione è che, in molti casi e in modo improprio, le norme sulla protezione dei dati vengano erroneamente viste come uno scudo all'esplicarsi del corretto esercizio della libertà di informazione. Questo spiega l'infondatezza di numerose pretese di cui sono testimonianza *provvedimenti* quali quello del 23 luglio 2009 [doc. *web* n. 1639507] relativo al contestato contenuto di alcuni articoli di stampa dedicati ad un noto personaggio calcistico. In tale decisione il Garante ha, peraltro, ripercorso e precisato i parametri normativi che delimitano, rispetto all'attività giornalistica, il proprio ambito di intervento. Si è così richiamata l'attenzione sulle disposizioni del Codice (artt. 136 *ss.*) che, al fine di contemperare i diritti della persona (in particolare quelli alla riservatezza) con il diritto di cronaca e di critica, prevedono specifiche garanzie nel caso di trattamenti svolti proprio a fini giornalistici. Tali trattamenti possono essere effettuati anche senza il consenso dell'interessato, sempre che si svolgano nel rispetto del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

Questi princìpi generali trovano poi uno spazio di specificazione e integrazione nelle disposizioni del codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica del 1998. Di tale codice, nella decisione citata, viene in rilievo in particolare il dettato dell'art. 6, sia in riferimento ai più ampi margini di cui

dispongono i giornalisti in rapporto a vicende che coinvolgono persone note, sia in relazione al disposto del comma 3 del medesimo art. 6, che ricorda come *"commenti e opinioni del giornalista appartengono alla libertà di parola e di pensiero costituzionalmente garantita a tutti"*. Ciò tenendo conto che non spetta al Garante valutare gli eventuali profili penali ravvisabili.

Interessante anche la *decisione* del 10 dicembre 2009 [doc. *web* n. 1691407] concernente la contestata pubblicazione dell'immagine della figlia minore di un noto personaggio televisivo. Nel caso di specie le supposte ragioni di tutela della minore non hanno trovato accoglimento atteso che l'istruttoria svolta ha appurato come l'immagine della bambina era già stata volontariamente resa nota al pubblico dagli stessi genitori, tanto da risultare reperibile sulla rete internet oltre che essere già stata pubblicata da altre testate giornalistiche, in contesti nei quali il genitore non solo ne aveva rivelato l'identità (oltre ad altri particolari), ma non aveva neanche preteso che ne venisse anonimizzato il volto.

Va infine ricordato il *provvedimento* 14 gennaio 2010 [doc. *web* n. 1701618] che affronta il sempre più attuale tema delle modalità di raccolta e successiva diffusione dei dati nell'ambito dei programmi televisivi che propongono inchieste su temi "delicati" attraverso raccolte di immagini e testimonianze ad insaputa degli interessati. Anche in questo caso vi è un importante riferimento nel codice deontologico che, dopo aver affermato che in linea di principio il giornalista deve rendere nota la propria identità e le finalità della raccolta, evitando artifici e pressioni indebite, fa comunque salva l'ipotesi che ciò possa non avvenire quando il rispetto di tali parametri di correttezza *"renda .... impossibile l'esercizio della funzione informativa"*. Nel *provvedimento* in oggetto, si è ammessa, in sede di raccolta delle immagini, la possibilità di riprendere particolari luoghi di incontro di persone con modalità atte a celare appunto la presenza di una *troupe* televisiva, ma si è invece riconosciuta la legittimità dell'opposizione, proposta da una delle persone riprese, alla successiva diffusione della propria immagine (senza oscuramento del volto) al momento della trasmissione del filmato. Ciò tenuto anche conto del fatto che la persona non era nota e la sua identificazione era irrilevante con riferimento alle finalità informative del servizio.

18. Il contenzioso giurisdizionale

18.1. Considerazioni generali

Anche nel 2009 è stata confermata l'utilità per gli interessati 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 centoventisette ricorsi del 2008 sono stati trattati dall'Autorità duecentotre ricorsi non coinvolgenti direttamente pronunce del Garante, di cui centoquarantasei relativi a giudizi proposti nel 2009.

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 dal'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 il ruolo 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. I 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 2008, nel corso del 2009 l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

Con sentenza n. 5198 del 3 settembre 2009 il Consiglio di Stato ha confermato la

sentenza con la quale il Tribunale amministrativo regionale del Lazio aveva accolto il ricorso di una società che gestisce un sistema di informazione creditizia avverso il silenzio-rifiuto serbato dal Garante sull'istanza intesa ad ottenere l'emanazione degli atti di cui all'art. 10, comma 8, del Codice. Il Consiglio di Stato ha stabilito che il Garante, sull'istanza della società, ha l'obbligo di avviare un procedimento amministrativo al fine di verificare l'esistenza dei presupposti, indicati direttamente dal legislatore, che rendano necessario il versamento del contributo da parte dell'interessato, e per determinarne l'ammontare.

Avverso tale sentenza il Garante ha proposto ricorso per Cassazione per motivi attinenti alla giurisdizione.

Non si sono, inoltre, riscontrate pronunce che hanno dichiarato un difetto di competenza per materia.

In tema di competenza territoriale il Tribunale di Milano (sentenza n. 2534 del 24 febbraio 2009) e il Tribunale di Roma (sentenza n. 4868 del 4 marzo 2009) in applicazione del disposto di cui all'art. 152, comma 2, del Codice, hanno dichiarando la propria incompetenza territoriale a conoscere delle controversie ivi azionate in favore del tribunale del luogo dove risiede il titolare del trattamento (rispettivamente il Tribunale di Bologna e il Tribunale di Milano).

È giunto a conclusione il procedimento introdotto dal ricorso straordinario al Presidente della Repubblica nei confronti del *provvedimento* 23 gennaio 2008 ([doc. *web* n. 1487903], *v. Relazione 2007*, p. 117), con il quale l'Autorità ha disposto nei confronti del Consiglio dell'ordine degli avvocati di Santa Maria Capua Vetere il divieto del trattamento, in qualunque forma, di dati personali biometrici di alcuni praticanti avvocati. Confermando il precedente orientamento (Sez. prima n. 4468/2007, *v. Relazione 2008*, p. 210), il Consiglio di Stato ha dichiarato il ricorso inammissibile (Ad. Prima Sezione n. 3754 del 13 maggio 2009). Pur ricordando che la giurisprudenza dello stesso Consiglio ha ritenuto ammissibile in via di principio, avverso gli atti amministrativi illegittimi, sia il ricorso straordinario al Presidente della Repubblica, sia l'azione avanti al giudice ordinario, il Consiglio ha però escluso la possibilità di

ricorso straordinario avverso gli atti dell'amministrazione oggetto di forme di tutela giurisdizionale, quale quella prevista dall'art. 152, comma 1, del Codice, qualificabile come esclusiva e funzionale.

18.3. I PROFILI DI MERITO

Alcune pronunce emesse dall'autorità giudiziaria, in fattispecie in cui non erano in discussione provvedimenti adottati dal Garante, hanno fatto applicazione dell'art.137 del Codice, in tema di bilanciamento tra l'esercizio del diritto di cronaca e il diritto alla tutela dei dati personali.

In particolare tre decisioni hanno accertato la violazione del corretto esercizio del diritto di cronaca con riferimento al mancato rispetto del principio dell'essenzialità dell'informazione.

Con la prima, emessa dal Tribunale di Mantova (sentenza n. 789 del 10 luglio 2009), è stato ritenuto effettuato in violazione di detto principio il trattamento dei dati personali della vittima di un fatto delittuoso, della quale erano stati riportati su un quotidiano locale, oltre il nome e il cognome, anche il paese di residenza, l'indirizzo completo e l'esatta denominazione della ditta ove prestava lavoro. Il Tribunale, pur riconoscendo l'esistenza dell'interesse pubblico alla conoscenza della notizia, ha ritenuto non essenziale al fine della piena comprensibilità del fatto la pubblicazione dei predetti dati personali dell'interessato.

Un caso analogo è stato affrontato dal Tribunale di Como (sentenza n. 406 del 17 marzo 2009), che ha riconosciuto che i dati personali della vittima di una rapina pubblicati su un quotidiano locale (nome, cognome, residenza, composizione del nucleo familiare, professione) risultavano obiettivamente inutili e sovrabbondanti rispetto alla cognizione del fatto di cronaca da parte del pubblico, anche con riferimento all'art. 6 del codice deontologico relativo al trattamento dei dati personali nello svolgimento dell'attività giornalistica.

Il Tribunale ha anche condannato la società editrice del quotidiano, il direttore responsabile e il giornalista autore dell'articolo al risarcimento dei danni causati all'interessato.

Una terza decisione, emessa dal Tribunale di Genova (sentenza n. 1749 del 23 aprile 2008), ha riguardato la diffusione su un giornale locale dei dati (nome, cognome, età, professione, luogo di residenza e amministrazione comunale di servizio) dell'interessato, destinatario di una condanna in sede penale. Anche in tal caso il giudice ha riconosciuto non esservi in concreto un'utilità sociale alla conoscenza dei dati personali riguardanti il condannato, prevalendo la salvaguardia della dignità della persona, come prevista anche dal menzionato codice deontologico. Anche in tal caso il direttore responsabile del quotidiano è stato condannato a risarcire il danno al ricorrente.

Al contrario, il Tribunale di Milano ha ritenuto legittima la pubblicazione su di un quotidiano nazionale di notizie di carattere economico-patrimoniale su un investitore privato, nominativamente individuato, che aveva acquisito una quota di partecipazione in una società quotata in borsa. In tale caso il giudice ha ritenuto che i dati diffusi, esposti nel rispetto anche del principio di continenza, fossero indispensabili per fornire ai lettori un'informazione completa sulla vicenda (sentenza n. 15018 del 15 dicembre 2009).

18.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2009 ha registrato un netto incremento delle opposizioni a provvedimenti del Garante: a fronte dei trentadue ricorsi del 2008, sono state trattate sessantanove opposizioni, di cui cinquantasei proposte nel 2009. Di queste, diciassette si riferiscono a opposizioni ad ordinanze ingiunzioni, con un leggero aumento rispetto al 2008, nel quale si erano registrate quattordici opposizioni di tale natura.

Causa principale del complessivo incremento del contenzioso va ascritto ai giudizi promossi avanti al Tribunale di Roma da una nota società che gestisce alcune banche dati contenenti informazioni sui soggetti censiti estratte da altri archivi (detenuti per lo più da soggetti pubblici) per fornire alla propria clientela servizi aventi contenuto sia informativo, sia valutativo nell'ambito della *cd. "business information"*.

La casistica indica dodici opposizioni di tale natura (nel 2008 se ne era registrata solo una); di queste, undici sono state proposte avverso provvedimenti adottati su ricorso dell'interessato. Tutti i provvedimenti hanno ad oggetto l'utilizzo e l'accostamento ai

soggetti censiti di informazioni ritenute dal Garante ad essi non pertinenti. Undici giudizi sono giunti a definizione in sede di merito.

Il Tribunale di Roma si è espresso emettendo alcune pronunce favorevoli all'Autorità (sentenza n. 22836 del 6 novembre 2009; sentenza n. 20875 del 14 ottobre 2009; sentenza n. 11147 del 28 luglio 2009; sentenza n. 23198 del 18 febbraio 2010) ed altre sfavorevoli (sentenza n. 22833 del 6 novembre 2009; sentenza n. 13437 del 12 novembre 2009; sentenza n. 22476 del 3 novembre 2009; sentenza n. 24978 del 2 dicembre 2009; sentenza n. 19829 del 29 settembre 2009, sentenza n. 24978 del 1° dicembre 2009).

Un'opposizione ha riguardato il *provvedimento* 30 ottobre 2008 [doc. *web* n. 1570327] con il quale il Garante, tenuto conto dei numerosi ricorsi e segnalazioni pervenuti, ha vietato in via generale alla predetta società l'accostamento ai soggetti censiti di informazioni ad essi non pertinenti. Il Tribunale di Roma (sentenza n. 21109 del 16 ottobre 2009) ha accolto l'opposizione sulla considerazione che il provvedimento è stato adottato solo nei confronti della società ricorrente e non anche di tutti gli altri operatori del settore dell'informazione commerciale.

Complessivamente l'Autorità ha avuto notizia di trentasei decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi.

Otto pronunce concernono opposizioni a ordinanze ingiunzioni. Di queste, tre decisioni hanno avuto a oggetto violazioni dell'art. 13 del Codice per omessa o tardiva informativa agli interessati (Tribunale di Roma, sentenza n. 9297 del 29 aprile 2009 e sentenza n. 20467 dell'8 ottobre 2009; Tribunale di Trani, sentenza n. 2978 del 3 settembre 2009); due decisioni la violazione dell'art. 181 del Codice (Tribunale di Foggia, sentenza n. 618 del 9 aprile 2009; Tribunale di Crotone, sentenza n. 667 del 20 novembre 2009); una decisione l'omessa notificazione del trattamento con le modalità previste dall'art. 37 del Codice (Tribunale di Roma, sentenza n. 10093 del 13 maggio 2009). Tutte queste pronunce hanno respinto le opposizioni, confermando i provvedimenti del Garante.

Sul rispetto dei termini per la notificazione dell'atto di contestazione della violazione

amministrativa in un caso il Tribunale di Torino ha accolto il ricorso proposto da una società automobilistica (sentenza n. 4685 del 29 giugno 2009), in un altro il Tribunale di Piacenza si è invece espresso in senso favorevole all'Autorità (sentenza n. 363 del 19 maggio 2009).

In materia di diffusione dei dati su internet, un'associazione di consumatori ha proposto opposizione avverso il *provvedimento* 6 maggio 2008 [doc. *web* n. 1512255] che ha dichiarato illegittima la diffusione dei redditi dei contribuenti da parte dell'Agenzia delle entrate sul proprio sito internet. Il Tribunale di Roma (sentenza n. 964 del 16 gennaio 2009) ha dichiarato cessata la materia del contendere in considerazione dell'entrata in vigore del d.l. n. 112/2008, convertito nella l. n. 133/2008.

Due pronunce hanno riguardato l'esercizio del diritto di accesso a documenti detenuti dal Garante. In entrambi i casi il Tribunale amministrativo regionale del Lazio ha respinto i ricorsi, sia per l'assenza di un interesse qualificato dei ricorrenti all'accesso ai documenti, sia per l'esistenza del diritto alla riservatezza dei dati ivi contenuti (sentenza n. 5586 del 12 giugno 2009 e sentenza n. 20 del 24 settembre 2009).

Per quanto attiene al trattamento di dati personali effettuato in ambito giornalistico, devono essere segnalate due pronunce relative al medesimo caso nel quale l'Autorità ha vietato l'ulteriore pubblicazione, su di un settimanale, di immagini di un noto uomo politico fotografato all'interno del parco di una sua proprietà. Al riguardo il Tribunale di Milano nel 2008 si era già espresso sulla vicenda per la parte di sua competenza, respingendo l'opposizione proposta dalla società editrice del settimanale (*v. Relazione 2008*, p. 213).

Il Tribunale di Tempio Pausania, sezione distaccata di Olbia, competente per territorio in ordine alle opposizioni proposte dall'agenzia giornalistica e dal fotografo, dapprima (sentenza n. 114 dell'8 maggio 2009) ha dichiarato l'inammissibilità del ricorso avverso il provvedimento del Garante di blocco della pubblicazione del materiale fotografico, del quale non è prevista l'impugnabilità, attesa la sua temporaneità e provvisorietà, se non unitamente alla decisione finale di merito (art. 150 del Codice).

Successivamente, ha respinto il ricorso proposto contro il *provvedimento* del 13

settembre 2007 [doc. *web* n. 1620926] con il quale l'Autorità ha vietato l'ulteriore pubblicazione delle immagini (sentenza n. 115 del 19 maggio 2009).

Condividendo gli argomenti espressi dal Garante, fatti propri anche dal giudice milanese, il Tribunale ha ritenuto nella specie illecita l'acquisizione delle immagini pubblicate per contrasto con norme del Codice e del codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica: il fotografo aveva infatti violato il domicilio dell'interessato - dovendosi ritenere il parco quale pertinenza dell'abitazione - utilizzando mezzi tecnici particolarmente invasivi, costituiti da potenti teleobiettivi.

In materia di trattamento di dati giudiziari si è avuta notizia di due decisioni emesse dalla Suprema Corte di Cassazione, entrambe favorevoli al Garante (relative ai *provvedimenti* del 13 novembre 2003 e del 7 luglio 2005) attinenti, l'una, alla produzione in giudizio di una lettera contenente dati riguardanti il ricorrente, che è stata ritenuta esente da censure (sentenza n. 3358 dell'11 febbraio 2009), l'altra, all'acquisizione, valutata corretta tenuto conto delle competenze istituzionali dell'organo, da parte del Consiglio dell'Ordine degli avvocati di Rimini dei dati giudiziari del ricorrente, al fine di verificare la permanenza dei requisiti per l'iscrizione nel registro dei praticanti avvocati (sentenza n. 22423 del 22 ottobre 2009).

Un'altra pronuncia della Corte di Cassazione (sentenza n. 4207 del 28 gennaio 2009) ha accolto il ricorso dell'Aci e confermato il *provvedimento* dell'8 novembre 2002, cassando la sentenza del Tribunale di Roma. La Corte ha affermato che il diritto dell'interessato all'annotazione della variazione anagrafica sul Pra, fondato sull'art. 13 della l. n. 675/1996, non comporta la gratuità della prestazione da parte dell'ente gestore del pubblico registro.

Altre due decisioni hanno riguardato il trattamento dei dati da parte di ordini professionali.

Nel primo caso il Garante, con *provvedimento* 30 aprile 2008, aveva riconosciuto a un ingegnere il diritto all'integrazione delle informazioni conservate presso gli archivi dell'Inarcassa con i dati relativi al proprio domicilio.

Il Tribunale di Roma (sentenza n. 23771 del 19 novembre 2009) ha respinto

l'opposizione, condividendo integralmente le argomentazioni del Garante.

Nel secondo caso il Garante, con *provvedimento* 13 novembre 2008 [doc. *web* n. 1519536] aveva rigettato l'istanza di un architetto che chiedeva la cancellazione dal sito internet dell'Ordine degli architetti della Provincia di Bergamo della notizia di provvedimenti disciplinari a suo carico. Il Tribunale di Bergamo (sentenza n. 822 dell'8 aprile 2009), in linea con quanto disposto dall'Autorità, ha rigettato il ricorso sulla base dell'art. 61 del Codice, che consente espressamente la diffusione di tali dati.

Altre due pronunce hanno avuto a oggetto lo svolgimento del procedimento amministrativo avanti al Garante.

Con entrambe le decisioni sia il Tribunale di Milano (sentenza n. 15016 del 15 dicembre 2009), sia il Tribunale di Firenze (sentenza n. 202 del 26 gennaio 2009) hanno respinto le opposizioni proposte nei confronti rispettivamente dei *provvedimenti* del 14 novembre 2003 [doc. *web* n. 1121183] e del 30 aprile 2008 [doc. *web* n. 1515623] con cui il Garante ha dichiarato non luogo a provvedere sui ricorsi degli interessati a seguito dell'adesione spontanea alle richieste dei ricorrenti intervenute nel corso del procedimento da parte dei titolari del trattamento. Con le sentenze l'autorità giudiziaria ha riconosciuto il pieno rispetto da parte dell'Autorità del dettato dell'art.149 del Codice in tema di svolgimento e conclusione del procedimento amministrativo.

Due decisioni hanno riguardato la *delibera* del Garante n. 46 del 26 giugno 2008 attinente le *"Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero"* [doc. *web* n. 1534086].

In entrambi i casi il Tribunale di Bassano del Grappa (sentenza n. 334 del 12 maggio 2009) e il Tribunale di Roma (sentenza n. 19883 del 2 ottobre 2009) hanno dichiarato inammissibili i ricorsi rilevando l'assenza di interesse ad agire in capo ai ricorrenti per difetto di una concreta e attuale lesione di un loro interesse giuridicamente qualificato, non avendo le linee-guida contenuto precettivo ma essendo esplicazione del potere conferito all'Autorità di curare la conoscenza della disciplina in materia di trattamento dei dati personali (art. 154, comma 1, lett. *h*), del Codice).

In tema di *marketing* si registra una sola sentenza, con cui il Tribunale di Ferrara,

confermando il *provvedimento* del Garante del 26 luglio 2006 [doc. *web* n. 1323119], ha respinto l'opposizione proposta da una società assicurativa che aveva effettuato, nei confronti dei ricorrenti, telefonate promozionali senza consenso (sentenza del 15 luglio 2009).

Infine, è stato respinto il ricorso proposto davanti al Tribunale di Roma avverso il *provvedimento* del Garante del 1° marzo 2007 [doc. *web* n. 1387522] in tema di trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori.

Il Tribunale, dopo aver riconosciuto la sussistenza del potere del Garante di adottare provvedimenti di carattere generale aventi contenuto prescrittivo e inibitorio (art. 154, comma 1, lett. *c*) e *d*), del Codice), ha ritenuto legittime le indicazioni indirizzate dal Garante ai datori di lavoro di adottare alcune misure, necessarie e opportune, per conformare alle disposizioni vigenti il trattamento dei dati personali effettuato per verificare il corretto utilizzo, da parte dei dipendenti nell'ambito del rapporto di lavoro, della posta elettronica e della rete internet (sentenza n. 12826 del 19 gennaio 2010).

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, 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.

19. L'ATTIVITÀ ISPETTIVA E LE SANZIONI

19.1. LA PROGRAMMAZIONE DELL'ATTIVITÀ ISPETTIVA

Nel 2009 sono state effettuate quattrocentoquarantanove ispezioni (quattrocentoventicinque delle quali sulla base dei programmi ispettivi semestrali disposti dall'Autorità).

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, 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);
- società che effettuano trattamenti di dati personali facendo ricorso a nuove tecnologie (*ad es.*, mediante identificazione a radiofrequenza *Rfid*) o, comunque attraverso internet (*ad es.*, commercio *online*);
- 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).

Sul piano procedimentale occorre evidenziare che 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 indirizzi, 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 *Newsletter* settimanale pubblicata sul sito *www.garanteprivacy.it.*

L'attuazione dell'attività ispettiva da parte dell'Ufficio permette di acquisire significativi 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 2009, il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, fosse indirizzata a:

- trattamenti di dati personali effettuati dall'amministrazione finanziaria mediante il sistema informativo della fiscalità (anagrafe tributaria);
- 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 in ambito sanitario relativamente alla legittimità della consultazione e del successivo utilizzo di dati da parte di soggetti aventi diritto, nonché alle misure di sicurezza adottate.

Con riferimento, invece, al periodo luglio-dicembre 2009, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- trattamenti di dati personali effettuati dall'amministrazione finanziaria mediante il sistema informativo della fiscalità (anagrafe tributaria);
- trattamenti di dati personali effettuati da enti previdenziali mediante i propri sistemi informativi;
- 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*.

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.

Occorre aggiungere, per completezza, che 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 relativi alle 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 d'intesa siglato nel 2005.

Il consolidato rapporto con il Corpo consente al Garante di disporre di risorse qualificate in grado di supportare l'attività ispettiva sull'intero territorio nazionale attraverso:

- la partecipazione di personale agli accessi alle banche dati, ispezioni, verifiche

e alle altre rilevazioni nei luoghi ove si svolge il trattamento;

- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività ispettive delegate o subdelegate per l'accertamento delle violazioni;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori;
- la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

A tal fine la Guardia di finanza ha previsto, nell'ambito del Comando Unità Speciali, un apposito reparto, il Nucleo speciale *privacy* con sede a Roma, che provvede direttamente ad effettuare gli accertamenti, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Qualora nell'ambito dell'ispezione emergano violazioni penali o amministrative, la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'autorità giudiziaria e alla contestazione della sanzione amministrativa.

Sono proseguite, anche nel 2009, le attività tese a realizzare un maggior coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, gruppi, compagnie e tenenze) e a rafforzare il ruolo di coordinamento del Nucleo speciale *privacy* rispetto all'attività subdelegata a tali reparti. L'obiettivo è quello di disporre di un dispositivo di controllo flessibile ed articolato che consenta, in funzione della complessità degli accertamenti, di effettuarli direttamente a cura del Dipartimento ispettivo dell'Ufficio, ovvero attraverso il Nucleo speciale, oppure, nel caso di accertamenti di non elevata complessità che concernono, ad esempio, la verifica di singoli adempimenti, delegando anche i reparti territoriali della Guardia di finanza.

Al fine di migliorare costantemente il livello qualitativo degli accertamenti delegati al Corpo, vengono mantenuti continui contatti col personale addetto ai controlli e sono stati svolti incontri con funzionari del Garante esperti in specifici settori nonché mirate attività formative a beneficio degli appartenenti al Nucleo speciale *privacy*.

19.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2009 sono state effettuate, suddivise per settore, le seguenti attività ispettive:

- settanta controlli nei confronti di cliniche private e ospedali e case di cura pubbliche che trattano dati relativi alla salute, con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza;
- sessanta nei confronti di aziende municipalizzate per la raccolta dei rifiuti, per la distribuzione di gas metano e acqua, con riferimento alla liceità del trattamento dei dati degli utenti;
- trentacinque controlli nei confronti di aziende che forniscono beni e servizi, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- trenta controlli nei confronti di aziende di trasporto pubblico, con riferimento alla liceità del trattamento dei dati dei clienti;
- ventisei controlli nei confronti di società che effettuano selezioni di persone per la partecipazione a programmi televisivi (*casting*), con riferimento alla liceità dei trattamenti dei dati degli aspiranti alla selezione;
- venticinque controlli nei confronti di società che forniscono servizi sportivi, con riferimento ai trattamenti dei dati dei clienti;
- venti controlli nei confronti di aziende che gestiscono porti turistici, con riferimento alla liceità del trattamento dei dati dei clienti;
- venti controlli nei confronti di aziende che hanno notificato al registro generale dei trattamenti la costituzione di banche dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni e a comportamenti illeciti o fraudolenti;

- quindici controlli nei confronti di aziende autorizzate dall'Amministrazione autonoma dei monopoli di stato all'esercizio dei giochi pubblici a distanza (scommesse), con riferimento alla liceità del trattamento dei dati degli interessati che si registrano per poter giocare via *web*;
- dieci controlli nei confronti di aziende che gestiscono impianti di risalita presso le più importanti località sciistiche, con riferimento alla liceità dei trattamenti dei dati dei clienti, in particolar modo in relazione all'impiego di sistemi identificazione a radiofrequenza *Rfid*;
- dieci controlli nei confronti di farmacie, con riferimento alla liceità del trattamento dei dati dei clienti;
- tredici 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;
- dieci controlli nei confronti di società che forniscono banche dati a terzi per finalità di *marketing* telefonico e postale, volti a rilevare la liceità del trattamento con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati per tali finalità;
- nove controlli nei confronti di gestori di servizi di comunicazione elettronica, in relazione al rispetto dei termini e delle modalità di conservazione dei dati di traffico telefonico e telematico nonché all'attività di profilazione dei clienti.

A questi si aggiungono i novantasei controlli effettuati nei confronti di altri soggetti in relazione alle 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 è stato prescritto ad un condominio che aveva

installato un sistema di videosorveglianza di commisurare il tempo di conservazione delle immagini alle effettive finalità della raccolta (nel caso di specie, allo stato degli atti, per un intervallo temporale non superiore alle quarantotto ore) e di rendere l'informativa nelle aree esterne sottoposte a videosorveglianza, mediante opportuna segnaletica riportante il *modello semplificato di informativa* "minima" (*Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]);

- il *provvedimento* con il quale il Garante ha disposto il blocco del trattamento effettuato mediante alcune videocamere poste in aree suscettibili di transito da parte dei lavoratori, come quelle di carico e scarico delle merci, i *box* informazioni e la zona circostante. Il sistema di videosorveglianza può, infatti, configurarsi come forma di controllo a distanza dell'attività lavorativa anche nel caso in cui i luoghi di lavoro siano frequentati anche solo temporaneamente dal personale (*Provv.* 26 febbraio 2009 [doc. *web* n. 1601522]);
- il *provvedimento* con il quale il Garante ha vietato ad una società, specializzata nella vendita *online* di biglietti per eventi musicali, teatrali, sportivi e culturali e che opera su internet, l'ulteriore trattamento dei dati personali dei clienti acquisiti in assenza di una chiara informativa e di richieste di consenso differenziato in relazione alle diverse finalità perseguite dalla società (*Provv.* 5 marzo 2009 [doc. *web* n. 1615731]);
- il *provvedimento* con il quale il Garante ha vietato ad una società il trattamento di qualunque dato personale effettuato tramite l'utilizzo del telefax per l'invio di comunicazioni promozionali a terzi senza che risulti la prova documentata di aver acquisito il consenso preventivo, specifico e informato degli interessati ai sensi dell'art. 130 del Codice (*Provv.* 22 maggio 2009 [doc. *web* n. 1621185]);
- il *provvedimento* con il quale il Garante ha prescritto ad una società bancaria di adottare misure di sicurezza idonee, consistenti nell'assicurare la tempestiva disattivazione di credenziali di autenticazione attribuite alla clientela, al fine di contenere il rischio di accesso non autorizzato (*Provv.* 28 maggio 2009 [doc. *web* n. 1624668]);

- il *provvedimento* con il quale il Garante ha vietato ad una società l'ulteriore comunicazione a terzi, non aventi titolo, di dati personali relativi alla situazione debitoria riferita agli interessati. (*Provv.* 28 maggio 2009 [doc. *web* n. 1624760]);
- il *provvedimento* con il quale l'Autorità ha ordinato ad una società operante nel settore tessile di cancellare i dati personali dei titolari della carta fedeltà "non pertinenti e eccedenti" (professione dei richiedenti e tutti i dati riferiti ai figli chiesti, fin dal 2000, con la compilazione del modulo) rispetto all'unica attività perseguita con l'utilizzo della *card*, consistente nell'attribuire sconti presso i punti vendita che commercializzano il proprio marchio (*Provv.* 28 maggio 2009 [doc. *web* n. 1625257]);
- il *provvedimento* con il quale il Garante ha vietato l'uso, in forma centralizzata, dei dati biometrici raccolti da un importante centro orafo e ha imposto alla società che gestisce la struttura di adeguare anche il sistema di videosorveglianza e gli altri trattamenti dei dati personali alla normativa (*Provv.* 4 giugno 2009 [doc. *web* n. 1629975]);
- il *provvedimento* con il quale il Garante ha prescritto ad una società che promuove, attraverso procacciatori di affari, la vendita di "punti vacanza" che consentono all'acquirente l'utilizzo, per un determinato periodo di tempo, di alloggi siti in complessi immobiliari ubicati fuori dal territorio italiano, l'integrazione della modulistica contenente l'informativa da fornire alla propria clientela e la designazione per iscritto dei procacciatori di affari come incaricati del trattamento dei dati ai sensi dell'art. 30 del Codice, impartendo ai medesimi le relative istruzioni (*Provv.* 4 giugno 2009 [doc. *web* n. 1630006]);
- i *provvedimenti* con i quali il Garante ha disposto il divieto nei confronti di alcune società dell'ulteriore trattamento dei dati biometrici dei dipendenti per la finalità di rilevazione delle presenze dei lavoratori (*Provv.* 12 giugno 2009 [doc. *web* n. 1635731]; *Provv.* 15 ottobre 2009 [doc. *web* n. 1664257]; *Provv.* 29 ottobre 2009 [doc. *web* n. 1682066]);
- il *provvedimento* adottato, in relazione agli accertamenti effettuati a seguito di una

segnalazione, riguardante il trattamento illecito dei dati personali del segnalante da parte della propria banca (*Provv.* 18 giugno 2009 [doc. *web* n. 1635720]);

- il *provvedimento* generale con il quale il Garante ha stabilito le regole alle quali ci si dovrà attenere per un corretto uso dei dati personali a fini di profilazione nel settore delle telecomunicazioni (*Provv.* 25 giugno 2009 [doc. *web* n. 1629107]);
- il *provvedimento* con il quale il Garante, ritenuto illecito il trattamento di dati personali effettuato presso istituto bancario da un incaricato, ha prescritto di adottare idonee misure organizzative e idonee misure di sicurezza tese sia a garantire la scrupolosa vigilanza sull'operato degli incaricati, sia a sensibilizzare gli stessi incaricati al rispetto delle istruzioni ricevute in occasione di iniziative formative (*Provv.* 23 luglio 2009 [doc. *web* n. 1640294]);
- il *provvedimento* con il quale il Garante ha prescritto ad una compagnia aerea internazionale di riformulare l'informativa da rendere agli interessati, con riferimento al trattamento effettuato presso le biglietterie site nel territorio dello stato italiano nell'ambito del programma di fidelizzazione della clientela (*Provv.* 23 luglio 2009 [doc. *web* n. 1640398]);
- il *provvedimento* con il quale il Garante ha prescritto ad un patronato, quale misura opportuna, di designare quali responsabili del trattamento i soggetti operanti presso le proprie strutture regionali ai sensi dell'art. 29 del Codice (*Provv.* 2 ottobre 2009 [doc. *web* n. 1666101]);
- il *provvedimento* con il quale sono state impartite prescrizioni in relazione al trattamento dei dati nell'ambito del servizio di riscossione a mezzo ruolo (*Provv.* 7 ottobre 2009 [doc. *web* n. 1664231]);
- i *provvedimenti* con i quali l'Autorità ha vietato a tre società che operano nel settore della telefonia e internet il trattamento di dati per periodi di tempo superiori a quelli previsti dalla legge (*Provvedimenti* 19 novembre 2009 [doc. *web* nn. 1695393 e 1695368] *Provv.* 21 ottobre 2009 [doc. *web* n. 1683093]).

19.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

19.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

In conseguenza delle ispezioni effettuate, sono state inviate all'autorità giudiziaria quarantatre informative (di cui venti da parte del dipartimento attività ispettive e sanzioni dell'Autorità e ventitre da parte della Guardia di finanza).

Le violazioni penali hanno riguardato:

- mancata adozione delle misure minime di sicurezza (ventiquattro);
- trattamento illecito dei dati (sette);
- falsità nelle dichiarazioni e notificazioni al Garante (sei);
- mancato adempimento di un provvedimento del Garante (quattro)
- altre fattispecie (due).

Quattordici sono stati i procedimenti connessi al *cd. "ravvedimento operoso"* in materia di misure minime di sicurezza, previsto dall'art. 169, comma 2, del Codice.

Tale disposizione prevede, come noto, che nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure minime di sicurezza (Allegato B. al Codice) il Garante impartisca una prescrizione alla persona individuata come responsabile della predetta violazione e, verificato il ripristino delle misure violate, ammetta il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a trentamila euro). L'adempimento alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

19.4.2. Sanzioni amministrative

In conseguenza delle ispezioni effettuate, sono stati avviati trecentosessantotto procedimenti sanzionatori amministrativi (di cui duecentoventotto ad opera del Dipartimento e centoquaranta da parte della Guardia di finanza e altri organi accertatori).

Le sanzioni amministrative contestate hanno riguardato le seguenti violazioni:

- omessa o inidonea informativa (duecentotrenta);

- trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (settantacinque);
- omessa informazione o esibizione al Garante (trenta);
- omessa o incompleta notificazione (ventiquattro);
- inosservanza di un provvedimento del Garante (sei);
- sanzioni in materia di conservazione dei dati di traffico (una);
- più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (una);
- codice del consumo (una).

Sotto il profilo economico, le sanzioni contestate vanno complessivamente da un minimo di 3.643.516 euro a un massimo di 21.513.823 euro.

Il sostanzioso incremento dell'impatto economico delle sanzioni rispetto all'anno precedente è da ricollegarsi alle modifiche apportate all'apparato sanzionatorio amministrativo introdotte con il d.l. n. 207/2008, convertito nella legge 27 febbraio 2009, n. 41.

A fronte delle predette contestazioni sono stati definiti spontaneamente dalle parti, mediante l'oblazione in via breve o mediante ordinanza, circa centosettanta procedimenti ed effettivamente riscossi nell'anno 1.572.432 euro (in gran parte ancora relativi a procedimenti sanzionatori avviati prima delle modifiche introdotte con le norme di cui sopra).

Come evidenziano i dati, il maggior numero di sanzioni è da porre in relazione alla 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.

Al secondo posto, in termini di numero di contestazioni, si colloca una delle nuove sanzioni, prevista dall'art. 162, comma 2-*bis* del Codice; si tratta delle ipotesi di *"illecito trattamento amministrativo"* dei dati personali e di omissione nell'adozione delle misure minime di sicurezza. L'elevato numero di contestazioni è da ricondursi a violazioni relative al consenso al trattamento da parte dell'interessato, in tutti quei casi in cui la legge lo richieda come necessario, e alla mancata adozione delle misure di 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 norma, oltre alla contestazione della sanzione si procede ad un accertamento *in loco* al fine di acquisire i necessari elementi istruttori.

Da segnalare anche le prime applicazioni delle sanzioni previste per l'inosservanza dei provvedimenti del Garante (art. 162, comma 2-*ter*) e dall'art. 164-*bis*, comma 2, del Codice.

Quest'ultima norma introduce una nuova fattispecie aggravata nel caso in cui siano commesse più violazioni di un'unica o di più disposizioni sanzionate amministrativamente in relazione a banche dati di particolare rilevanza o dimensioni.

La disposizione prevede tre condizioni:

- la commissione di una pluralità di violazioni sanzionate amministrativamente, sia che le violazioni riguardino una stessa disposizione, sia che riguardino disposizioni diverse (*ad es.*, più omesse informative o un'omessa informativa e un'omessa notificazione o mancata adozione di misure di sicurezza);
- la circostanza che le violazioni di cui sopra siano commesse *"in relazione a banche dati"* (la nozione di banca dati è quella prevista dall'art. 4, comma 1, lett. *p*): *"qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti"*);
- la natura della banca dati che deve essere di particolare rilevanza o dimensioni.

19.4.3. L'apparato sanzionatorio e le disposizioni procedurali

Il d.l. n. 207/2008, convertito nella legge 27 febbraio 2009, n. 41, ha apportato significative modifiche all'apparato sanzionatorio del Codice. Le modifiche si sono concentrate, in massima parte, sulle sanzioni amministrative mentre è rimasto sostanzialmente inalterato l'impianto sanzionatorio penale.

In linea generale, gli interventi hanno comportato: un aumento delle pene pecuniarie previste per ciascuna violazione; la previsione di nuove ipotesi sanzionatorie; la creazione di meccanismi per consentire una maggiore modulabilità della sanzione in rapporto

al caso concreto in ragione della minore o maggiore gravità, della circostanza che le violazioni siano state commesse in relazione a banche di dati di particolare rilevanza o dimensioni, del coinvolgimento di un maggior numero di interessati e delle condizioni economiche del contravventore.

Fra le nuove fattispecie sanzionatorie amministrative sono state previste, all'art. 162, comma 2-*bis*, del Codice, le ipotesi di trattamento illecito e di omissioni nell'adozione delle misure minime di sicurezza (già sanzionate penalmente dagli artt. 167 e 169 del Codice, articoli tuttora vigenti).

La sanzione amministrativa (da 10.000 euro a 120.000 euro, come determinata dall'art. 20-*bis* del d.l. 25 settembre 2009, n. 135, convertito, con modificazioni, dalla legge 20 novembre 2009, n.166) può essere contestata in tutti i casi di violazione delle disposizioni richiamate dall'art. 167 nonché nei casi di violazione delle misure minime di sicurezza previste dal Codice e, per quanto riguarda le misure minime di sicurezza, senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta.

È stata inoltre introdotta, all'art. 162, comma 2-*ter*, una specifica fattispecie sanzionatoria amministrativa (da 30.000 euro a 180.000 euro) nei casi di inottemperanza ai provvedimenti del Garante che prescrivono, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti o che prevedono il blocco o il divieto del trattamento.

La norma rafforza la cogenza delle determinazioni dell'Autorità, in precedenza garantita, limitatamente alla violazione dei provvedimenti di blocco e di divieto del trattamento nonché di quelli relativi alla decisione dei ricorsi, dalla sanzione penale prevista dall'art. 170 del Codice.

Per quanto riguarda i meccanismi introdotti al fine di modulare le sanzioni amministrative, va evidenziato in primo luogo che l'art. 164-*bis*, comma 1, prevede la possibilità di contestare le sanzioni accertate applicando una riduzione a due quinti dei limiti minimo e massimo previsto per ciascuna violazione, nei casi di minore gravità della violazione stessa o in relazione alla natura economica e sociale dell'attività svolta dal contravventore.

Di contro, i commi 2 e 3 del medesimo articolo prevedono delle particolari "aggravanti" che determinano un sensibile aumento delle sanzioni:

- in caso di più violazioni di un'unica o di più disposizioni commesse, anche in tempi diversi, in relazione a banche di dati di particolare rilevanza o dimensioni (sanzione da 50.000 euro a 300.000 euro senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta);
- in altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, con aumento dei limiti minimo e massimo delle sanzioni previste per ciascuna violazione in misura pari al doppio.

Tutte le sanzioni possono essere, inoltre, ai sensi dell'art. 164-*bis*, comma 4, aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

Dalla data di notifica della contestazione della sanzione amministrativa decorrono i termini per inviare al Garante eventuali memorie difensive o chiedere l'audizione (trenta giorni) o per definire il procedimento in via breve mediante oblazione del doppio del minimo della sanzione prevista per la violazione (sessanta giorni).

In base a quanto previsto dall'art. 166 del Codice, l'organo competente a ricevere il rapporto e ad irrogare le sanzioni in materia di protezione dei dati personali è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni.

Le modalità e le competenze in relazione ai procedimenti sanzionatori amministrativi sono stabiliti dall'art. 16 del *Regolamento* n. 1/2007, così come modificato dalla *delibera* del 15 ottobre 2009.

Fuori dei casi in cui è effettuata dal personale operante in sede di controllo, la contestazione delle violazioni amministrative è adottata con atto sottoscritto dal dirigente del Dipartimento attività ispettive e sanzioni. Quando non è effettuato il pagamento in misura ridotta, lo stesso dirigente dispone, in conformità alla legge, l'eventuale archiviazione degli atti a seguito di idonee deduzioni difensive.

Nei casi in cui, invece, si renda necessario procedere all'applicazione della sanzione, il provvedimento che definisce il procedimento sanzionatorio (ordinanza-ingiunzione) è adottato dal segretario generale in caso di applicazione della sanzione in misura pari al minimo; in tutti gli altri casi, e, comunque, in caso di applicazione della sanzione prevista dagli articoli 162, comma 2-*bis*, 162, comma 2-*ter* e 163, ovvero qualora si applichi una delle ipotesi aggravate di cui all'art. 164-*bis*, dal Collegio.

Avverso le ordinanze-ingiunzione è ammesso, ai sensi dell'art. 152 del Codice, il ricorso in opposizione al Tribunale ordinario del luogo ove ha sede il titolare del trattamento, entro il termine di trenta giorni dalla notificazione del provvedimento.

20. LE RELAZIONI INTERNAZIONALI

Per quanto riguarda l'evoluzione del quadro delle relazioni comunitarie ed internazionali, l'evento principale e più atteso è senz'altro l'entrata in vigore, il 1° dicembre, del Trattato di Lisbona.

Con il Trattato la protezione dei dati personali acquista un nuovo e diverso ruolo. Il Trattato infatti richiama espressamente ed ingloba nel quadro giuridico europeo le disposizioni della Carta dei diritti fondamentali, che, com'è noto, all'art. 8 ha introdotto il diritto fondamentale delle persone alla tutela dei propri dati personali, affiancandolo all'art. 7 che riguarda il diritto alla riservatezza.

Trattandosi di un diritto fondamentale, cambia l'interpretazione degli strumenti giuridici adottati in materia: la Direttiva n. 95/46/CE, che contiene i princìpi armonizzati, esce definitivamente dal contesto in cui è nata - il mercato interno - per assumere pienamente il ruolo di strumento giuridico di riferimento per le istituzioni europee ogni volta che esse intendano legiferare su aspetti che possano avere un impatto sul diritto alla protezione dei dati. Quindi dovranno essere considerate e rispettate le disposizioni della direttiva non solo per i trattamenti di dati personali svolti nell'ambito di attività economiche, ma anche per quelli rientranti nel settore pubblico e finora considerati non coperti dal diritto comunitario.

Questa indicazione è ulteriormente rafforzata dal fatto che l'entrata in vigore del Trattato comporta la fine della divisione in pilastri dell'ordinamento comunitario e prevede che, in materia di trattamento dei dati personali, sia assicurato un quadro di riferimento tendenzialmente unico.

Finora, il quadro armonizzato di princìpi costituito dalla Direttiva n. 95/46/CE e dalla Direttiva n. 2002/58/CE valeva solo nell'ambito del *cd.* "primo pilastro" che, nel garantire la libera circolazione dei dati personali tra i paesi dell'Unione europea, assicurava agli individui un elevato livello di tutela. Nessun principio esiste al momento per quanto riguarda i trattamenti di dati che si svolgono nel *cd.* "secondo pilastro" (politica estera e di sicurezza comune), anche se il Trattato prevede l'adozione di specifiche regole.

Nel *cd.* "terzo pilastro" è stata adottata una decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che dovrà essere attuata dai paesi dell'Unione entro la fine di novembre 2010.

Tuttavia le sue disposizioni non sono rivolte a disciplinare i trattamenti di dati all'interno dei singoli paesi, ma solo a dettare regole comuni, peraltro ispirate al principio del minimo denominatore. Tali disposizioni sono state fortemente criticate dal Parlamento europeo e dalle autorità nazionali ed europee di protezione dei dati, soprattutto con riferimento al trasferimento di dati da un paese Ue ad un Paese terzo ed al successivo uso dei dati scambiati.

Un ulteriore e favorevole effetto dell'entrata in vigore del Trattato è dato dal maggiore ruolo riconosciuto al Parlamento europeo, che diviene un vero codecisore anche nell'area sopra indicata; ciò che favorisce l'interlocuzione con le autorità di protezione dei dati personali riunite nel Gruppo Art. 29 e nel *Working Party on Police and Justice* (*Wppj*). Sono già evidenti i primi effetti su alcuni accordi internazionali negoziati in settori particolarmente delicati: il Parlamento ha richiesto il parere delle autorità di protezione dei dati ed ha successivamente negato il suo appoggio all'accordo-ponte Ue-Usa per l'uso dei dati *Swift*, negoziato dal Consiglio e dalla Commissione e concluso proprio in concomitanza con l'entrata in vigore del Trattato. Situazioni analoghe si sono verificate per quanto riguarda gli accordi con Stati uniti, Australia e Canada concernenti l'uso dei dati personali dei passeggeri aerei.

Si tratta per lo più di accordi stipulati "a porte chiuse" senza il coinvolgimento del Parlamento europeo, che, almeno in Italia, non sono sottoposti a ratifica parlamentare né a consultazione del Garante. Anche in questo caso il Trattato, tramite il Protocollo sul ruolo dei Parlamenti nazionali, consentirà ad essi una partecipazione più attiva.

In parallelo alle attività legate all'entrata in vigore del Trattato di Lisbona, la Commissione europea ha aperto una stagione di riflessione sull'attualità dei princìpi della Direttiva n. 95/46/CE soprattutto in relazione alle sfide tecnologiche ed alla globalizzazione, lanciando una consultazione pubblica cui le autorità di protezione dei dati hanno voluto contribuire con un importante documento congiunto WP29 e *Wppj* sul futuro

della *privacy* (*v. par.* 20.2.) in cui, pur dando un giudizio di sostanziale tenuta delle regole, si sottolinea l'esigenza di migliorare l'applicazione della direttiva, rendendo effettivi i suoi princìpi e raggiungendo una applicazione realmente armonizzata. Il documento evidenzia tuttavia anche aspetti più critici, che richiedono una riflessione non limitata all'orizzonte europeo, come la disciplina dei flussi internazionali di dati e gli aspetti legati all'uso di nuove tecnologie (*Rfid, Cloud computing*).

In proposito, sia la risoluzione adottata nella Conferenza di primavera svoltasi il 23 e 24 aprile ad Edimburgo sia, in modo più corale ed ambizioso, la predisposizione ed adozione di una serie di princìpi definiti *"standard internazionali"* in materia di *privacy*, testimoniano l'impegno profuso dalle autorità per essere in prima fila nel dibattito, ed il loro ruolo proattivo rispetto all'individuazione di problemi e possibili soluzioni.

Un altro importante contributo fornito alla Commissione, al Parlamento ed al Consiglio dalle autorità europee di protezione dei dati ha riguardato l'adozione del nuovo programma quinquennale di lavoro in materia di polizia e sicurezza, il *cd. "programma di Stoccolma"*, per il quale si rinvia al paragrafo dedicato alla cooperazione nel settore libertà, sicurezza e giustizia.

L'attenzione delle autorità resta comunque ferma, come ben mostrano i pareri adottati dal Gruppo Art. 29 e dal *Wppj*, sul quadro giuridico generale esistente, per valutarne la tenuta e migliorarne l'attuazione ovvero per rendere più effettiva la cooperazione tra le autorità stesse, ad esempio, nello svolgimento di attività comuni di accertamento, come l'azione di *enforcement* del WP29 relativa alla direttiva sulla *data retention*, le altre svolte nell'ambito delle autorità comuni di controllo Schengen, EUROPOL, Dogane ed EURODAC, nonché l'adozione ed attuazione delle azioni indicate nel manuale dal *Wppj*.

Il Garante ha partecipato alle diverse attività menzionate, sia nei gruppi di lavoro sia in cooperazione tra e con le autorità europee e mondiali di protezione dei dati personali come sarà meglio descritto *infra*.

In alcuni casi ha anche svolto, come per il Gruppo di lavoro polizia e giustizia, un ruolo di stimolo e propositivo determinante, testimoniato dalla rielezione del presidente del Garante italiano alla sua direzione.

20.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Spring Conference 2009

Il 23 e 24 Aprile si è tenuta a Edimburgo la Conferenza di primavera delle autorità di protezione dei dati personali, dedicata a *"Come migliorare la protezione dei dati"* attraverso iniziative volte a rafforzare e rendere effettive le garanzie previste dalle norme vigenti. Prendendo spunto da un'analisi della Direttiva n. 95/46/CE e delle diverse ipotesi di revisione, i relatori hanno dibattuto sui punti di forza e debolezza della normativa attuale e sugli approcci sinora adottati per potenziarla. Il mutamento del contesto ha fatto sorgere problemi complessi di ridefinizione del significato della protezione dei dati, del tipo di regole effettivamente necessarie e del ruolo che devono svolgere le autorità per la *privacy* con riferimento alle nuove "sfide" tecnologiche e globali. La sessione presieduta dal presidente dell'Autorità italiana è stata dedicata agli obiettivi che l'attività dei regolatori deve porsi per garantire effettivamente la protezione dei dati a livello individuale e sociale.

Nella Dichiarazione finale i Garanti hanno evidenziato il patrimonio di esperienza e conoscenza che l'Europa può e deve apportare alla ricerca di soluzioni ed approcci sempre più condivisi per garantire la tutela dei dati personali a livello mondiale. La Dichiarazione ha evidenziato la necessità di guardare ai molti punti in comune che già contraddistinguono il quadro normativo europeo e internazionale. Ma soprattutto ha raccomandato ai soggetti coinvolti (pubblici, privati e istituzionali) di mettere a punto norme e *standard* che - a partire dai princìpi di protezione dati già affermati - siano in grado di garantire e promuovere i diritti e le libertà fondamentali; di sviluppare nelle tecnologie approcci che prevedano la *privacy* come elemento essenziale (*privacy by design*); di realizzare una efficace protezione dei dati personali tenendo in considerazione i rischi per i singoli e per la società nel suo complesso.

Nell'ambito della Conferenza ampio è stato il contributo fornito dal Gruppo di lavoro polizia e giustizia. In primo luogo è stato presentato ed approvato il rapporto di attività 2007-2008 del *Working Party on Police and Justice* (*Wppj*), e sono stati illustrati i risultati raggiunti e le iniziative future. Inoltre è stata adottata una risoluzione sugli accordi bilaterali e multilaterali stipulati fra paesi europei e non-europei in materia di cooperazione giudiziaria e di polizia (*cd.* "terzo pilastro").

Considerata l'esistenza di troppe difformità nelle garanzie fissate da tali accordi per quanto riguarda la protezione dei dati, i Garanti hanno chiesto agli Stati di garantire livelli uniformi di tutela anche attraverso l'inserimento di clausole-*standard* concernenti la protezione dei dati personali. La Conferenza ha anche adottato il "manuale" elaborato dal *Wppj* per definire alcuni criteri applicabili alle attività di ispezione e monitoraggio concernenti la materia del "terzo pilastro". La Conferenza ha infine rieletto all'unanimità per un secondo mandato il Presidente, prof. Francesco Pizzetti, dopo aver dato atto dell'importante lavoro svolto.

World Conference delle autorità di protezione dei dati

Dal 4 al 6 novembre 2009 si è svolta a Madrid la *31ma Conferenza internazionale delle autorità di protezione dei dati*, con la partecipazione di 50 Paesi. Fra i temi più rilevanti all'ordine del giorno devono essere ricordati: il contemperamento fra proprietà intellettuale e diritto alla *privacy* su internet; la ricerca del giusto equilibrio tra sicurezza, sorveglianza e libertà; la difesa dei minori riguardo all'uso dei loro dati personali soprattutto nei *social network*; i flussi internazionali di dati nel rispetto delle garanzie per i cittadini.

Il presidente dell'autorità italiana ha presieduto una specifica sessione dedicata alle soluzioni possibili per contemperare proprietà intellettuale, diritti delle imprese e tutela degli utenti.

Durante la Conferenza è stata approvata un'importante risoluzione sugli *standard* internazionali in materia di *privacy*, che contiene un primo pacchetto di regole e princìpi condivisi a livello mondiale.

Attraverso gli *standard* vengono definiti una serie di princìpi, diritti, obblighi e meccanismi procedurali che ciascun ordinamento è chiamato ad assicurare in tema di *privacy* e protezione dei dati, nel settore pubblico e in quello privato.

I princìpi condivisi possono essere così sintetizzati: liceità, correttezza e proporzionalità del trattamento di dati personali; rispetto del principio di finalità; trasparenza dei trattamenti; qualità e sicurezza dei dati; salvaguardia dei diritti di accesso, rettifica, cancellazione e opposizione da parte degli interessati; responsabilità del titolare anche per i trattamenti affidati a soggetti esterni; rafforzamento delle tutele per i dati sensibili; obbligo di assicurare il rispetto di questi *standard* nei trasferimenti internazionali di dati;

garanzia di un controllo indipendente affidato ad autorità autonome ed imparziali provviste di adeguati poteri e risorse; potenziamento di approcci proattivi e preventivi basati sull'impiego di tecnologie, su valutazioni preventive di impatto-*privacy*, su controlli di qualità. Secondo la risoluzione, gli *standard* potranno costituire un'utile base di partenza per promuovere l'ulteriore armonizzazione delle garanzie in materia di *privacy*, soprattutto per quanto riguarda i flussi internazionali di dati. I princìpi generali a tutela della protezione dei dati riaffermati nella risoluzione hanno il pregio di poter essere accettati anche da autorità di Paesi non Ue che hanno una diversa cultura della protezione dei dati, favorendo in tal modo una tutela globale.

Tra le altre significative risoluzioni approvate dalla Conferenza figurano quella sulla tutela della *privacy online* dei minori e quella sulla creazione di un sito *web* della Conferenza internazionale per favorire la circolazione internazionale dei documenti e delle informazioni in materia di protezione dati.

Nel corso della Conferenza è stato attribuito ad Ilita (Autorità israeliana per la tutela dei dati personali) lo *status* di membro della Conferenza ed è stata accettata la candidatura di Israele per l'organizzazione della prossima conferenza mondiale.

Altre conferenze

Il 14 maggio 2009 si è tenuta a Bruxelles una importante conferenza *"Towards the Evaluation of the Data Retention Directive"* in cui si è avuto il primo confronto fra i centoquaranta partecipanti appartenenti a tutti i settori interessati (autorità di *law enforcement*, autorità di protezione dati, settore privato, *ong*) relativamente all'attuazione della Direttiva n. 2006/24/CE e in particolare alla valutazione prevista dall'art. 14 entro il 15 settembre 2010.

Sempre a Bruxelles il 19-20 maggio 2009 si è tenuta una conferenza organizzata dalla Commissione europea, dal titolo: *"Personal Data: More Use, More Protection?"* volta a raccogliere stimoli e suggerimenti ai fini della consultazione pubblica lanciata dalla Commissione sullo stato di attuazione della Direttiva n. 95/46/CE e sull'eventuale opportunità di una sua revisione. La Conferenza intendeva approfondire il tema della protezione dei dati nel mondo globalizzato e alla luce delle nuove tecnologie, con particolare riferimento ai temi dell'accesso ai dati da parte di autorità pubbliche e soggetti privati,

dei flussi di dati transfrontalieri nel *cd. "cloud computing"* e delle aspettative degli individui, del mondo del *business* e della società nel suo complesso rispetto alle tematiche in esame. Il presidente dell'Autorità è intervenuto nella sessione sul diritto all'oblio. Dopo aver rappresentato il quadro normativo, internazionale ed europeo, in cui può essere rintracciato tale diritto, ha mostrato come le nuove tecnologie abbiano contribuito all'emersione di nuove dimensioni dell'oblio, favorendo la dispersione del controllo da parte dell'interessato sulla propria sfera informativa. A tal proposito, il Prof. Pizzetti ha ricordato la tematica dei motori di ricerca e della particolare difficoltà di cancellare i dati personali (anche dalla copia *cache*), facendo riferimento alle decisioni dell'autorità italiana in materia di archivi *online* dei giornali e di pubblicazione delle decisioni di autorità pubbliche. Ha concluso ripercorrendo le sfide rappresentate dalla nuove tecnologie, sottolineando la necessità di sviluppare un nuovo approccio fondato su princìpi armonizzati a livello internazionale.

20.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

L'attività del Gruppo Art. 29 si è orientata secondo le tre linee fondamentali individuate nel programma di lavoro adottato per il biennio 2008-2009: miglioramento dell'efficacia delle disposizioni contenute nella Direttiva n. 95/46/CE, studio dell'impatto delle nuove tecnologie e sviluppo di una visione globale (trasferimenti internazionali di dati e impatto della globalizzazione). Rientra nel primo obiettivo il lavoro di interpretazione della Direttiva n. 95/46/CE soprattutto con riferimento alle nozioni di *"data controller"* e di *"data processor"*. L'analisi, approfondita nell'ambito di uno specifico gruppo di lavoro, è sfociata in un testo che, oltre a meglio determinare gli elementi caratterizzanti delle diverse figure, ne specifica le singole peculiarità in vista dell'allocazione della responsabilità, dell'individuazione dei rispettivi ruoli in caso di attività di *outsourcing*, nonché delle ipotesi di contitolarità del trattamento. In tale linea, è stato inoltre approfondito il concetto di *"legge applicabile"* per meglio definire l'ambito di applicazione della normativa europea in materia di protezione dei dati personali, soprattutto in relazione ai trattamenti che assumono carattere transnazionale. L'obiettivo è quello di individuare

i "confini" della normativa in questione, anche al fine di semplificare gli oneri gravanti su operatori aventi sedi dislocate in diversi Stati membri dell'Ue.

Il sottogruppo specificamente dedicato all'attività di *enforcement* ha proseguito nella verifica dell'applicazione della Direttiva n. 2006/24/CE alla conservazione dei dati a fini di lotta alla criminalità. Come anticipato nella *Relazione 2008* (*cfr.* pag. 244), le Autorità degli Stati membri hanno provveduto ad inviare un identico questionario alle società fornitrici di reti e servizi di comunicazioni elettroniche. Alcuni Paesi, compatibilmente con i poteri attribuiti alle singole autorità, hanno poi effettuato anche ispezioni *in situ*, per verificare la correttezza delle informazioni ricevute. All'esito di queste attività ciascuna Autorità ha redatto un *National Report* evidenziando lo stato dell'arte in ciascun Paese e le maggiori criticità. I risultati complessivi saranno sintetizzati in un documento adottato dalla Assemblea Plenaria del WP29 che rivolgerà le raccomandazioni agli operatori del settore e potrà essere tenuto in considerazione dalla Commissione in vista della valutazione prevista dall'art. 14 della Direttiva n. 2006/24/CE entro il 15 settembre 2010.

Altrettanto intenso è stato il lavoro condotto in materia di nuove tecnologie. Particolare attenzione è stata rivolta all'utilizzo dei *social network*, alle attività di trattamento poste in essere dai motori di ricerca (in particolare con riferimento ai tempi e alle modalità di conservazione dei dati), al servizio fornito da *Google Street view*. Il lavoro di approfondimento è stato arricchito da audizioni dei titolari del trattamento e ha condotto all'individuazione di specifiche raccomandazioni in materia. Analoga attenzione hanno suscitato le tematiche legate alle attività del *cd. "marketing comportamentale"*, soprattutto in considerazione del massiccio uso, in questo settore, di attività di profilazione degli utenti.

Con riferimento ai trasferimenti internazionali di dati il Gruppo, su richiesta della Commissione europea, si è espresso positivamente sull'adeguatezza delle legislazioni di Andorra ed Israele in materia di protezione dei dati. Intensa, inoltre, è stata la riflessione in materia di *binding corporate rules*, che ha prodotto buoni risultati in termini di accelerazione dei tempi di definizione della procedura europea di cooperazione tra autorità. Analoga attenzione è stata rivolta al settore delle *Standard contractual clauses*, mediante un

parere, espressamente richiesto dalla Commissione europea, sullo schema di proposta volto alla definizione di un nuovo set di clausole da titolare a responsabile.

Il Gruppo ha, inoltre, affrontato le tematiche delle centrali rischi pubbliche e private (con particolare riferimento alle attività di trattamento poste in essere da società di informazione creditizia) ed ha dato mandato al sottogruppo *Financial Matters* di approfondire l'impatto sulla protezione dei dati personali e sulla *privacy* delle disposizioni delle direttive europee adottate in materia di anti riciclaggio e prevenzione dell'uso del denaro per finanziare il terrorismo. Il sottogruppo ha inoltre contribuito a predisporre il parere, adottato dal WP29 congiuntamente al *Wppj*, inviato al Parlamento europeo in relazione allo schema di accordo ponte Eu-Usa sull'uso dei dati di messaggistica finanziaria (*Swift*), accordo successivamente rifiutato dal Parlamento.

Continua e costante attenzione è stata anche mantenuta, attraverso in particolare i lavori del sottogruppo *Traveller Data*, riguardo al trattamento dei dati dei passeggeri aerei in relazione ad accordi sull'uso di tali dati da parte di Paesi terzi (Australia, Canada, Stati Uniti) e ai problemi derivanti dall'introduzione del programma *e-Borders* nel Regno Unito, con le richieste di fornire in anticipo dati dei passeggeri colà diretti anche in relazione a voli intracomunitari ovvero a trasporti terrestri e marittimi (*Eurotunnel*).

Il Gruppo, sempre basandosi sui lavori del sottogruppo, ha fornito le sue osservazioni in merito all'introduzione dei *body scanner* negli aeroporti ed ha anche adottato un parere sul trattamento dei dati nell'ambito dei *duty free shop* presenti negli aeroporti.

Infine, il Gruppo ha partecipato, insieme al Gruppo polizia e giustizia, all'importante consultazione pubblica lanciata dalla Commissione europea in materia di *"Future of privacy"*, attraverso la definizione di un documento che, nel ribadire la validità dell'impianto normativo di base assicurato dalla direttiva del 1995, auspica l'introduzione di innovazioni in grado di potenziare e rendere più effettiva la tutela del diritto alla protezione dei dati personali.

Parere 5/2009 sui *social network online*

Con il parere in argomento il Gruppo Art. 29 ha chiarito che il mondo dei *social network* (*Sn*) non è sottratto alle tutele che la Direttiva n. 95/46/CE prevede rispetto al trattamento di dati personali. Gestori e utenti di questi servizi hanno specifiche

responsabilità, che il parere individua fornendo indicazioni in ordine alla legge applicabile, alla titolarità del trattamento e alle informazioni che devono essere date agli interessati.

Il Gruppo ha affermato, in particolare, che i gestori di tali piattaforme, anche di quelle gestite da Paesi extra-Ue, sono soggetti alle disposizioni della direttiva (e, quindi, delle leggi nazionali in materia), nella misura in cui il funzionamento dei *Sn* richieda l'utilizzo di "strumenti" situati fisicamente sul territorio dell'Ue (compresi i *cookie* che i *Sn* utilizzano per gestire la navigazione da parte degli utenti).

Si ricorda, inoltre, che il modello commerciale prevalente per i *social network* si basa sulla pubblicità presentata agli utenti, in maniera mirata, in base alle informazioni contenute nei profili-utente. Tutto ciò comporta numerosi trattamenti di dati personali e la necessità di una efficace tutela.

Particolare attenzione è stata dedicata all'individuazione del titolare del trattamento, che può identificarsi con il fornitore del servizio di *social network* e congiuntamente, a determinate condizioni, con l'utente che fruisce del servizio medesimo. Gli uni e gli altri hanno dunque specifiche e diverse responsabilità; per quanto riguarda i gestori, il documento ricorda gli obblighi di informativa agli utenti (i quali devono essere edotti sui rischi legati alla circolazione, talora inconsapevole, delle informazioni collocate nel proprio profilo), di conservazione limitata dei dati utilizzati per scopi amministrativi (*ad es.*, per aprire o chiudere un *account*), di messa a disposizione di strumenti efficaci per l'esercizio dei diritti degli utenti (accesso, rettifica), diritti che devono essere riconosciuti anche ai terzi i cui dati finiscano in un profilo *Sn*.

Fra le specifiche responsabilità degli utenti, prima fra tutte vi è quella di chiedere il consenso delle persone i cui dati siano fatti circolare, soprattutto se il numero di contatti e "amici" è particolarmente elevato e le informazioni non circolano all'interno di un gruppo chiuso. Sono indicati anche alcuni nodi problematici, come quello della verifica del consenso espresso dai minori, che costituiscono una fetta consistente degli utenti di questi servizi; sul punto il documento individua una possibile strategia basata su più strumenti (educazione, sensibilizzazione, soluzioni tecnologiche, autoregolamentazione), pur non nascondendo la difficoltà di trovare una risposta univocamente efficace.

Contributo alla consultazione pubblica del *DG MARKET* sul *report* dell'*Expert Group* in materia di *Credit Histories* (WP 164)

La Commissione aveva dato mandato ad un gruppo di esperti di approfondire, attraverso la predisposizione di un *report* poi sottoposto a consultazione pubblica, alcune tematiche in materia di circolazione e diffusione a livello europeo dei profili di credito che trovano largo impiego in particolare nell'ambito del credito al consumo.

Nel partecipare alla consultazione, il gruppo ha rilevato che il *report* non teneva nel debito conto i diritti degli interessati e, più in generale, non rifletteva in misura sufficiente gli obblighi derivanti dalla Direttiva n. 95/46/CE; il fatto che non in tutti Paesi dell'Ue esistano norme settoriali specifiche o codici di condotta che disciplinino la materia alla luce dei princìpi di protezione dati impone alla Commissione europea una particolare attenzione al fine di assicurare un approccio armonizzato e rispettoso dei diritti degli interessati. Le maggiori criticità, a giudizio del gruppo, riguardano la necessità di assicurare il diritto ad una informazione completa e precisa sulle finalità di utilizzo dei dati contenuti nei profili di credito, nonché il diritto d'accesso e di rettifica che dovrà essere esercitato gratuitamente soprattutto in considerazione della disponibilità di forme di accesso *online*. Nel *report* manca, inoltre, un'indicazione univoca sui dati che possono essere oggetto di trattamento per le finalità sottese alla creazione di questi profili; è chiaro che si tratta di un elemento essenziale per garantire un uso proporzionato e responsabile delle informazioni raccolte in base ai princìpi di proporzionalità e finalità, anche se sul punto emergono numerose divergenze fra le prassi e le norme nazionali. Anche la portata delle decisioni automatizzate dovrà essere ristretta, guardando al principio affermato nell'art. della Direttiva n. 95/46/CE, in particolare per quanto riguarda le conseguenze derivanti dall'attribuzione dei "punteggi" (*credit score*).

Adeguatezza del livello di protezione dei dati in Israele e Andorra (WP 165 e WP 166)

Su richiesta della Commissione europea, il Gruppo Art. 29 ha valutato il livello di protezione dei dati esistente in Israele e nel Principato di Andorra, giungendo in entrambi i casi ad un giudizio di adeguatezza, ai sensi dell'art. 25(6) della direttiva. Nei due Paesi esiste infatti un quadro di garanzie che, pur se operanti in modo diverso, nel complesso consentono il trasferimento di dati personali dall'Ue. In Israele, in particolare, vige un regime "misto" di *common law* e di tradizione continentale, per cui accanto ad una legge nazionale in materia (*Privacy Protection Act* del 1981) esistono *"Basic Laws"* che

sanciscono alcuni princìpi fondamentali (quali il principio di "proporzionalità" nell'attività di ogni soggetto pubblico o privato) oltre a precedenti giurisprudenziali che hanno fissato e ampliato questi princìpi anche con riguardo alla protezione dei dati. In Andorra vige invece un sistema di diritto continentale, con una legge del 2003 in materia di protezione dei dati personali che soddisfa sostanzialmente tutti i requisiti fissati nella direttiva, anche se con alcune eccezioni (compensate, peraltro, da altre normative settoriali). In entrambi i Paesi esistono autorità indipendenti incaricate di assicurare il rispetto della normativa, e il dibattito in corso (anche a livello parlamentare) sembra andare nella direzione di un ulteriore potenziamento della capacità di controllo e monitoraggio di tali autorità.

Parere 8/2009 sui dati dei passeggeri raccolti e trattati dai negozi *duty free* negli aeroporti e nei porti (WP 167)

Il Gruppo Art. 29 si è pronunciato con un parere sulle modalità di raccolta e utilizzo dei dati all'interno dei *cd.* "negozi *duty free*". Tali modalità sono risultate differenti tra gli Stati membri, e le direttive di riferimento relative al regime generale delle accise (92/12/CEE e successiva 2008/118/CE) non contengono alcun riferimento alla protezione dei dati personali nell'esercizio delle attività di *duty free.*

Al fine di avere una maggiore uniformità nella raccolta e nel trattamento dei dati, il Gruppo ha richiamato i negozi *duty free* negli aeroporti e nei porti ad applicare i princìpi della Direttiva n. 95/46/CE. Fermo restando l'attività di raccolta e conservazione dei dati riguardanti il regime di sospensione delle accise delle autorità doganali, regolate dalla Direttiva n. 2008/118/CE, il Gruppo ha ribadito, tra l'altro, che i passeggeri devono essere adeguatamente informati sulla raccolta, conservazione dei dati e finalità del trattamento e che tale raccolta deve essere limitata alla verifica del diritto all'esenzione delle imposte all'acquisto – e in nessun caso può essere utilizzata a fini di polizia.

Nel parere il Gruppo ha inoltre precisato che non deve essere possibile la raccolta e l'analisi dei dati al fine di identificare i comportamenti d'acquisto e che il periodo di conservazione dei dati deve essere uniforme per tutti gli Stati membri e limitato alla finalità di esenzione dell'accisa.

Contributo alla consultazione pubblica sul futuro della protezione dati (WP 168)

Il Gruppo Art. 29 ed il *Working Party on Police and Justice* hanno messo a punto congiuntamente un documento per rispondere alla consultazione pubblica aperta dalla Commissione europea nel luglio 2009 sul futuro della protezione dei dati come diritto

fondamentale. Il punto di vista delle autorità europee per la protezione dei dati è che l'impianto normativo di base assicurato dalla direttiva del 1995 sia ancora valido. E' tuttavia auspicabile che il legislatore europeo introduca alcune innovazioni e modifiche per rendere ancora più effettivo il diritto fondamentale alla protezione dei dati, ormai parte integrante del Trattato di Lisbona. In questa cornice dovrebbero essere ripensati alcuni concetti-chiave, come il consenso (che deve essere realmente libero ed informato), e dovrebbe essere sviluppato un quadro normativo unico che abbracci tutti gli ambiti nei quali si effettuano trattamenti di dati personali, compresi i trattamenti per finalità giudiziarie o di polizia.

Nel documento si chiede agli Stati nazionali di garantire che il diritto alla protezione dei dati sia rispettato anche quando il dato è trattato fuori dall'Unione europea, favorendo quindi la definizione di *standard* internazionali in materia, sul modello di quelli recentemente adottati dalla Conferenza internazionale di Madrid. Allo stesso tempo si chiede alla Commissione di fare chiarezza sugli *standard* di "adeguatezza" dei Paesi terzi ove si intendono trasferire i dati e di promuovere strumenti quali le "norme vincolanti d'impresa" con il supporto delle autorità nazionali di protezione dati.

Significativo è il richiamo alla necessità di garantire che i diritti di cui godono gli interessati siano esercitabili in modo semplice ed efficace: l'introduzione di *"class action"* (azioni collettive), un accesso più facile a rimedi di natura giudiziaria, sistemi alternativi per la risoluzione delle controversie, sono alcune delle proposte avanzate dalle autorità europee.

Viene proposta anche l'introduzione di un obbligo giuridico per i titolari di dimostrare di avere adottato tutte le misure previste dalla legge, trasformando la protezione dei dati in un elemento intrinseco e portante dell'organizzazione interna, sia in ambito pubblico che privato.

Largo spazio viene dedicato nel documento alle attività di cooperazione fra le autorità di protezione dati, con particolare riguardo alle "sfide" che attendono la protezione dati nell'area del cosiddetto "terzo pilastro". In questi ultimi anni, la cooperazione in materia giudiziaria e di polizia ha visto un forte potenziamento degli strumenti giuridici e tecnici finalizzati a consentire scambi di dati sempre più pervasivi ed estesi, senza che

a ciò si accompagnasse un ripensamento ed un'armonizzazione degli strumenti e delle norme a tutela della sfera privata dei cittadini. Su questo punto i garanti europei hanno chiesto ai legislatori europei e nazionali di invertire la tendenza, sviluppando un quadro giuridico armonizzato ed unificato, come previsto del resto anche nel *"programma di Stoccolma"* presentato dal Consiglio europeo dello scorso dicembre, in modo da muoversi nell'ottica del Trattato di Lisbona.

Altri documenti adottati dal Gruppo Art. 29

Si è riferito nella *Relazione 2008* (p. 139) dell'audizione dei principali gestori di motori di ricerca, da parte del WP29, sulle problematiche sorte a seguito del parere 4 aprile 2008 (WP 148) in materia di protezione dati, in relazione alle attività dei motori stessi (*cfr. Relazione 2007*, p. 164). Nel mese di ottobre il WP29 ha inviato a ciascun gestore le proprie osservazioni tramite lettere *ad hoc*. Le risposte, che daranno conto anche dell'adempimento alle indicazioni fornite dal WP29, saranno rese pubbliche.

Consultazione pubblica sull'impiego dei *body scanner* negli aeroporti - risposta del Gruppo Art. 29

Il WP29 nel mese di febbraio ha risposto alla consultazione pubblica lanciata dalla Commissione in materia di impiego dei *body scanner* negli aeroporti (*v.* Risoluzione del Parlamento europeo del 23 ottobre 2008 sull'impatto delle misure di sicurezza aerea e dell'impiego di *body scanner* sui diritti umani, la vita privata, la dignità personale e la protezione dei dati).

I Garanti europei, che su tale tema hanno lavorato in stretta collaborazione con l'EDPS (*European data protection supervisor*) hanno evidenziato una posizione fortemente critica rispetto all'impiego dei *body scanner*, soprattutto in relazione al principio di necessità, non essendo chiaro perché tali tecnologie dovrebbero garantire maggiormente la sicurezza rispetto all'utilizzo dei sistemi esistenti (perquisizioni manuali, *metal detector*).

Il Gruppo ha fatto presente che deve essere fatto un bilanciamento tra la necessità ed efficacia di tali sistemi e il loro impatto sulla *privacy* dei passeggeri. La Commissione, pur ribadendo il proprio interesse all'utilizzo di tale tecnologia, ha preso nota di tali posizioni critiche, espresse peraltro anche dal Parlamento europeo. La nuova proposta di regolamento sull'aviazione civile eviterà ogni riferimento all'utilizzo di tale strumento, e conterrà una disposizione che individui in maniera dettagliata le tipologie e le modalità di controllo dei passeggeri consentite.

Attualmente è stata costituita, presso la Commissione europea, una *Task force* sull'utilizzo dei *body scanner* (a cui partecipano anche il Gruppo Art. 29 e l'EDPS) al fine di definire un rapporto che determini una posizione comune in tutti gli Stati membri; l'Unione europea ha infatti rinviato l'adozione delle misure attinenti all'utilizzo dei *body scanner* in tutti gli aeroporti dell'Unione, in attesa di maggiori dettagli sugli aspetti legati all'efficacia, ai rischi per la salute e alla compatibilità con le libertà individuali.

Va ricordato che in Italia a metà febbraio è stato dato il via libera alla sperimentazione dei *body scanner* in alcuni aeroporti (Malpensa, Fiumicino, Venezia). In particolare, nei voli diretti in Usa saranno sperimentati due tipi di *body scanner*: quello a onde millimetriche e quello a raggi infrarossi.

Trattamento dei dati dei passeggeri

Sono continuate con impegno le attività relative al tema del trattamento dei dati dei passeggeri aerei, anche attraverso l'azione del sottogruppo *Traveller Data.* Alcune di queste attività sono state già ricordate come, ad esempio, il parere adottato in materia di trattamento dei dati nei *duty free shop* ed il contributo in merito all'introduzione di *body scanner* negli aeroporti.

Pnr Usa: nel corso della visita alla sede di *Amadeus,* l'unico dei quattro sistemi di prenotazione e gestione dei voli operanti a livello mondiale situato in territorio europeo, sono emersi alcuni aspetti che rendono necessario ed urgente verificare come gli Usa adempiono agli impegni assunti nell'Accordo stipulato nel 2007.

Sono quindi continuate le pressioni per l'attuazione della visita negli Usa per la revisione congiunta dell'applicazione degli Accordi, che si è finalmente svolta nel mese di febbraio 2010.

Alla revisione congiunta ha partecipato un rappresentante del WP29. Il sottogruppo *Traveller Data* ha contribuito alla predisposizione delle domande da sottoporre alla delegazione Usa. Nel frattempo il Gruppo ha espresso al Parlamento europeo, in risposta ad una richiesta del presidente della Commissione Libertà pubbliche, i dubbi e le perplessità maturate sui termini dell'Accordo, anche in vista di un suo rinnovo.

Analoghe lettere sono state inviate per quanto concerne gli Accordi per la trasmissione dei dati *Pnr* ad Australia e Canada, quest'ultimo peraltro scaduto.

Ciò deriva dall'esigenza, una volta entrato in vigore il Trattato di Lisbona, di sottoporre gli Accordi in vigore al Parlamento europeo; al riguardo la Commissione LIBE ha richiesto di conoscere il parere dei Garanti europei in relazione alla corrispondenza delle previsioni ivi contenute con i princìpi vigenti in materia di protezione dei dati personali e *privacy*.

Pnr europeo: i lavori sono stati congelati, anche se nel *"programma di Stoccolma"* viene riaffermata la volontà di pervenire all'adozione di un *Pnr* europeo, che peraltro potrebbe non essere limitato all'obbligo dei vettori aerei che operano voli verso il territorio europeo di trasmettere in anticipo i dati di cui man mano dispongono sulle intenzioni di viaggio, bensì anche comprendere voli intraeuropei e nazionali ed anche altri mezzi di trasporto terrestri e marittimi, in qualche modo seguendo il modello *e-Borders* introdotto dal Regno Unito anche come controllo integrato delle frontiere. Analoga sorte per la possibile introduzione di un sistema di autorizzazione preventiva al viaggio, sulla falsariga del sistema Esta introdotto dagli Stati Uniti.

Eborders: l'introduzione del sistema da parte delle autorità britanniche ha determinato l'obbligo per le compagnie aeree e per altri vettori marittimi e terrestri di trasmettere in anticipo rispetto all'effettuazione del viaggio i dati personali dei passeggeri, inizialmente limitati ai dati registrati al momento delle operazioni di imbarco (*cd. "Api"*).

Tutte le compagnie, incluse quelle operanti voli diretti nel Regno Unito dagli altri Paesi dell'Unione, sono state richieste a pena di sanzione di "partecipare al programma". Ciò ha avuto immediate ripercussioni con richieste inviate al Garante ed alle omologhe autorità garanti europee di conoscere se questo avrebbe o meno violato le disposizioni nazionali in materia di protezione dei dati personali.

Il Garante e molte altre autorità, alla luce del diritto nazionale e delle disposizioni adottate in attuazione della Direttiva n. 95/46/CE, hanno valutato non esistere una idonea base giuridica ed hanno chiesto alla Commissione europea di studiare gli aspetti della questione, inclusa la possibile violazione del principio di libera circolazione affermato dal Trattato dell'Unione, in modo da trovare una soluzione comune. Finora la questione non è stata risolta.

20.3. LA COOPERAZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Nel periodo di riferimento si è confermato (*cfr. Relazione 2008*, p. 246) da un lato l'intensificarsi dei lavori del Gruppo di lavoro polizia e giustizia (*Wppj*) sotto la guida del presidente del Garante ed il crescente coordinamento con il Gruppo Art. 29 su tutti i temi con implicazioni più ampie della competenza di un singolo "pilastro" (in particolare dati dei passeggeri, dati delle transazioni finanziarie, dati delle comunicazioni elettroniche) e, dall'altro, il tentativo del Consiglio e della Commissione di proporre e legiferare secondo metodologie non corrispondenti al nuovo Trattato, entrato in vigore il 1° dicembre del 2009. Come già rilevato, questo ha comportato il riesame da parte del Parlamento europeo di tali iniziative, che in alcuni casi ne ha determinato la caducazione.

I Garanti europei, sia nel *Wppj* sia nel Gruppo Art. 29, intensificando la loro cooperazione, hanno definito le osservazioni in relazione al nuovo programma di lavoro quinquennale nel settore libertà, sicurezza e giustizia ed al futuro della *privacy* (*cd. "programma di Stoccolma"*) in rapporto soprattutto con il Parlamento europeo per sopperire seppur parzialmente alla mancanza di "momenti istituzionalizzati" di dialogo. Una corretta applicazione del Trattato di Lisbona dovrebbe comportare la creazione di tali momenti, indispensabili per monitorare l'effettività dell'affermarsi dei diritti alla protezione dei dati ed alla riservatezza come diritti fondamentali garantiti a chiunque si trovi sul territorio dell'Unione.

Di grande utilità ed interesse è stata la partecipazione ai lavori del gruppo di esperti creato dalla Commissione per seguire l'applicazione della direttiva sulla conservazione dei dati di traffico a fini di prevenzione e repressione dei reati (*cd. "direttiva data retention"*) anche tenendo conto della parallela azione di *enforcement* varata dal Gruppo Art. 29. Questa attività ha consentito di definire alcuni documenti di lavoro volti a chiarire alcuni aspetti della direttiva per renderne più facile una applicazione uniforme - quali, ad esempio, il ruolo dei fornitori di transito internet (*Internet transit provider*), le obbligazioni per il filtraggio dello *spam*, l'applicazione della direttiva alla messaggistica *web* (*web mail* e *web based messaging*), il concetto di telefonia internet - nonché di partecipare

pienamente al processo di valutazione della direttiva stessa, che la Commissione dovrà completare entro il 15 settembre 2010.

Va menzionato poi che nel "terzo pilastro", a parte l'attività del Gruppo polizia e giustizia, è continuata l'attività degli organismi di supervisione e controllo comuni istituiti da specifiche Convenzioni (in particolare le Autorità comuni di controllo Schengen, EUROPOL e Dogane) e che dal 1° gennaio 2010 EUROPOL opera con una nuova base giuridica; per quanto riguarda invece la cooperazione doganale, sono state adottate nuove basi giuridiche che prevedono l'istituzione di una supervisione coordinata sul modello SIS II per le attività del *cd.* "primo pilastro" ed il mantenimento dell'Acc Dogane per quelle del "terzo pilastro".

E' continuata anche l'attività di supervisione a livello europeo sul funzionamento del sistema EURODAC, coordinata dall'EDPS. Sotto il profilo giuridico, la Commissione ha presentato delle proposte di modifica che, in particolare, consentono l'accesso al sistema EURODAC anche alle autorità di contrasto nazionali ed all'EUROPOL; su tali aspetti le autorità di protezione dei dati personali, attraverso pareri e comunicati stampa, hanno espresso forti critiche.

Working Party on Police and Justice (Wppj)

L'attività del *Working Party on Police and Justice* è proseguita nel 2009 secondo le priorità individuate nel programma di lavoro 2008-2009 (*v. Relazione 2008*, pag. 254); nel corso dell'anno si sono tenuti quattro incontri plenari, mentre il lavoro dei sottogruppi costituiti per la trattazione dei singoli temi ha consentito di elaborare posizioni, documenti e lettere tese a manifestare il punto di vista e le richieste delle autorità europee in tutte le sedi istituzionali opportune. E' stato inoltre definito il programma di lavoro per il successivo biennio 2010-2011, fissando alcuni obiettivi a breve ed a medio termine anche alla luce dell'entrata in vigore del Trattato di Lisbona e dei contenuti del *"programma di Stoccolma"* (adottato dal Consiglio europeo del 10/11 dicembre 2009).

Più in particolare, dopo l'adozione della decisione quadro in materia di protezione dati nel "terzo pilastro" (2008/977/GAI), e in vista della possibile entrata in vigore del Trattato di Lisbona, il *Wppj* ha costituito un gruppo ristretto che, riunitosi a Roma presso la sede dell'Autorità nel mese di settembre, ha definito le questioni organizzative, strategiche e di

sostanza sulle quali più urgente appariva un intervento delle autorità di protezione dati europee. In tale ambito si è stabilito di contribuire alla consultazione pubblica della Commissione europea sul *"futuro della protezione dati"* in Europa integrando il documento in preparazione da parte del sottogruppo *"Future of Privacy"* del WP29 (*par.* 20.2.) per gli aspetti più direttamente connessi alle attività del "terzo pilastro" nell'ottica dell'approvazione del Trattato di Lisbona; il *Wppj* ha ribadito la necessità di individuare forme nuove e più organiche di collaborazione con il WP29 e gli altri soggetti che si occupano di protezione dati a livello sopranazionale (comprese le autorità comuni di controllo nel "terzo pilastro").

Il *Wppj* ha ritenuto, in particolare, indispensabile addivenire ad un unico quadro giuridico che consenta di applicare anche alle questioni di "terzo pilastro" i princìpi fissati dalla Direttiva n. 95/46/CE, in linea con l'abolizione della distinzione fra pilastri della politica comunitaria fissata nel Trattato di Lisbona; ciò non esclude, comunque, la possibilità di introdurre strumenti specifici per disciplinare meglio le peculiarità legate alla cooperazione giudiziaria e di polizia (cosa prevista, del resto, dallo stesso Trattato).

Fa parte di tale obiettivo il lavoro di monitoraggio proseguito nel 2009 rispetto all'attuazione della decisione quadro 2008/977, pur essendo venuta a mancare l'occasione di un confronto pubblico con la Commissione europea e le altre istituzioni al fine di raccogliere *input* e suggerimenti da parte delle istituzioni maggiormente coinvolte (confronto che avrebbe dovuto tenersi nel mese di novembre 2009). Vanno anche ricordati, in tale contesto, i richiami rivolti dal *Wppj* alle istituzioni europee rispetto al proliferare di forme di svuotamento dei princìpi di protezione dati: in particolare in relazione alla proposta di modifica presentata dalla Commissione nel mese di settembre 2009 con riguardo al regolamento che disciplina EURODAC, tesa a consentire alle forze dell'ordine l'accesso alla relativa banca dati (che comprende informazioni sui richiedenti asilo nei Paesi Ue, istituita per finalità amministrative). In un comunicato stampa pubblicato il giorno in cui tale proposta è stata resa pubblica (10 settembre 2009), il *Wppj* ha ribadito la propria contrarietà a tale modifica, che contravviene alle finalità primarie della banca dati EURODAC e costituisce un pericoloso precedente.

Il settore dei flussi transfrontalieri di dati personali ha rappresentato naturalmente un importante banco di prova anche nel 2009. Occorre menzionare in tale contesto gli sviluppi intercorsi con riguardo ai flussi di dati fra Europa ed Usa, in particolare l'attività dello *"Eu-US High-Level Contact Group on Information Sharing and Privacy and Personal Data Protection"*. Tale gruppo di lavoro aveva elaborato una relazione finale (pubblicata con *addendum* nel mese di novembre 2009) in cui venivano fissati alcuni princìpi "condivisi" fra Ue ed Usa per quanto riguarda la tutela dei dati personali scambiati a livello transatlantico per la lotta al terrorismo ed altre gravi forme di criminalità. Il *Wppj* in precedenza aveva sollecitato il coinvolgimento delle autorità europee di protezione dati nell'attività di tale gruppo, senza alcun esito (due lettere erano state inviate nel 2008 e nel 2009 alle competenti istituzioni europee), ed ha quindi fatto presente la propria posizione (attraverso la presidenza italiana) in occasione dell'incontro convocato dalla Commissione europea, nel mese di febbraio 2010, per raccogliere suggerimenti e indicazioni dalle autorità di protezione dati, al fine della negoziazione di un eventuale accordo bilaterale in materia. Il *Wppj* ha anche deciso di contribuire alla consultazione pubblica che la Commissione ha lanciato nel mese di gennaio 2010 su questo stesso *dossier*. Restano da chiarire numerosi aspetti di tale accordo, ad iniziare dalla sua portata e dallo specifico contenuto dei princìpi di protezione dati in esso contenuti; resta fondamentale la questione dei meccanismi atti a garantire la tutela dei cittadini europei che ritenessero violati i propri diritti dal trattamento dei dati effettuato negli Usa. Le autorità europee di protezione dati hanno in programma di adottare una mozione sul punto in occasione della *Spring Conference 2010*.

Sempre con riferimento ai flussi transatlantici di dati, il *Wppj* ha anche approvato il testo di una lettera destinata ai ministeri nazionali competenti e concernente la stipula di accordi bilaterali cosiddetti *"simil-Prüm"* fra alcuni Stati europei (fra cui l'Italia) e gli Stati Uniti ai fini dello scambio di informazioni per finalità giudiziarie e di polizia (in particolare dati Dna), per sollecitare attenzione sulla necessità di rispettare alcuni princìpi essenziali in materia di tutela dei dati personali. Peraltro, si sono manifestate alcune problematiche legate alla corretta attuazione a livello nazionale delle disposizioni contenute nelle

decisioni di recepimento del Trattato di Prüm, sulle quali il *Wppj* ha chiesto chiarimenti al Consiglio Ue ed ai ministeri competenti (con particolare riguardo alle prassi relative agli artt. 3 e 4, comma 1, della decisione di attuazione del Trattato di Prüm 2008/615/GAI). Un altro delicato *dossier* nel 2009 ha riguardato i sistemi di messaggistica *Swift* (dati relativi alle transazioni bancarie), in particolare il progetto di accordo fra Ue ed Usa in materia; il *Wppj* ha redatto una lettera congiunta con il WP29, indirizzata alla Commissione LIBE del Parlamento europeo nel mese di gennaio 2010, per manifestare le proprie perplessità e critiche rispetto a numerosi punti di tale accordo (ad iniziare dalle diverse definizioni di "terrorismo" in ambito Ue ed Usa e dai meccanismi di revisione dell'accordo stesso).

Per quanto riguarda le attività già programmate, il *Wppj* ha completato la ricognizione dello stato dell'arte relativo agli accordi bilaterali con Paesi extra-europei in materia di cooperazione giudiziaria e di polizia, grazie ai contributi forniti dalle delegazioni nazionali, ed ha elaborato il testo di una clausola addizionale da inserire in tali accordi per fissare i princìpi fondamentali in materia di protezione dati, in ciò seguendo l'indicazione fornita dalla *Spring Conference* di Edimburgo nel 2009. La clausola (poi approvata nel mese di marzo 2010) prevede una doppia formulazione, con un diverso livello di dettaglio, per tenere conto del diverso quadro di garanzie derivante dall'eventuale adesione del Paese terzo alla Convenzione 108/81 del Consiglio d'Europa; in quest'ultimo caso, infatti, il Paese terzo è tenuto quanto meno al rispetto dei princìpi fondamentali fissati in materia attraverso la Convenzione.

E' stata completata anche l'analisi riferita allo stato di attuazione della Convenzione del Consiglio d'Europa concernente la criminalità informatica, in questo caso attraverso l'elaborazione di alcune raccomandazioni che saranno veicolate dalle autorità di protezione dati ai ministeri competenti negli Stati membri che devono ancora recepire la Convenzione stessa; esse rispecchiano alcune delle problematiche emerse dall'analisi degli strumenti di recepimento nazionale attualmente in essere.

Va infine ricordato che, dopo l'approvazione da parte della *Spring Conference* di Edimburgo del "Catalogo" in materia di supervisione e co-operazione elaborato dal *Wppj*,

è iniziata nel 2009 un'attività di *"risk assessment"* basato sui criteri fissati in tale "Catalogo"; l'obiettivo è l'individuazione di alcuni settori meritevoli di accertamenti ulteriori (eventualmente attraverso ispezioni congiunte) al fine di elaborare una politica organica di supervisione per il 2010-2011 e garantire il rispetto armonizzato dei princìpi di protezione dati fissati nella Convenzione 108/81 e nella Direttiva n. 95/46/CE. La *Spring Conference* 2010 è stata chiamata ad approvare l'elenco di tali aree di intervento dando mandato al *Wppj* di proseguire i necessari approfondimenti.

EUROPOL: l'attività dell'Autorità di controllo comune e i casi di contenzioso

A seguito della Decisione 2009/371/GAI del 6 aprile 2009 sull'integrazione di EUROPOL tra le strutture dell'Unione e sulla definizione del quadro generale di riferimento per lo svolgimento della sua attività e per le norme attuative della decisione medesima (entrata in vigore 1° gennaio 2010), che ha sostituito la Convenzione finora in vigore, gran parte dell'attività dell'anno è stata dedicata alla ridefinizione di tutte le norme collegate, in modo da adeguarle al nuovo quadro giuridico. Su molte di queste proposte l'Autorità comune di controllo è stata chiamata a rendere il suo parere. L'Acc ha anche adottato le necessarie modifiche al regolamento interno, nonché ridefinito il mandato dei suoi componenti e degli organi direttivi, nuovamente designati, procedendo poi alla rielezione/conferma di presidente e vicepresidente. È stato, inoltre, rinnovato il mandato per il gruppo ispezioni e confermato il coordinatore. L'ispezione annuale si è svolta come di regola nel mese di marzo ed il rapporto, che conferma l'importanza fondamentale delle stessa, è stato approvato.

Alcuni elementi emersi andranno approfonditi per valutarne la congruità con il quadro legale di EUROPOL, se del caso anche con azioni di verifica da svolgere a livello nazionale.

Mentre l'ispezione annuale consente infatti di monitorare attentamente la compliance di EUROPOL nei trattamenti di dati a quanto prescritto dalla Convenzione, sempre di più emergono scenari in cui l'acquisizione e la messa a disposizione di dati avvengono in un quadro meno chiaro.

Ad esempio, si prospetta un coinvolgimento di EUROPOL per quanto riguarda i reati finanziari (sullo sfondo della prospettiva dell'accordo Eu-Usa sui dati *Swift*), il fenomeno

dell'immigrazione e l'attività di *Frontex*.

Altro aspetto di grande importanza attiene all'attribuzione di credenziali per l'accesso ai vari *database* creati per fini di cooperazione tra forze di polizia per operare il *crosschecking* dei dati.

Al fine di disporre, nelle ispezioni, di una metodologia uniforme e risultati comparabili, si è deciso di curare la predisposizione di un modulo uniforme per le risposte da fornire in relazione agli specifici, puntuali accertamenti da svolgere a livello nazionale sulla base delle segnalazioni inviate dal *team* ispettivo e necessarie al completamento dell'ispezione annuale. Le questioni relative al modo in cui l'autorità di protezione dati nazionale esercita il suo ruolo di controllo verranno esaminate in un secondo tempo.

Sono stati adottati due pareri sul livello di adeguatezza di Macedonia e Colombia concludendo che non ci sono ostacoli all'apertura di un negoziato con questi Paesi al fine di poter stipulare con gli stessi un accordo operativo che consenta anche lo scambio di dati personali.

Occorre tuttavia che l'Acc si esprima con un nuovo parere sulle specifiche ed effettive garanzie di tale scambio.

Sono altresì proseguite le discussioni sul trattamento di dati personali e su possibili punti di contrasto tra la (nuova) base giuridica dell'EUROPOL ed altri strumenti in vigore, fra i quali la decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (*"iniziativa svedese"*, GU L 386, del 29 dicembre 2006).

Revisione della funzione delle decisioni costitutive

L'Acc ha valutato la funzione delle decisioni costitutive degli archivi di lavoro per fini di analisi. L'Autorità ha discusso la struttura delle decisioni costitutive, il loro ruolo e scopo come pure la loro funzione, sia interna che esterna. Ha inoltre esaminato l'esigenza di operare una distinzione netta tra la nozione di "dati comuni" e quella di "dati sensibili", le modifiche all'attuale *iter* di analisi criminale e infine, ma non meno importante, l'opportunità di aumentare la funzione di trasparenza delle decisioni costitutive.

Sul punto, l'Acc ha deciso di avviare delle discussioni con l'EUROPOL volte a

sondare, chiarire e risolvere eventuali divergenze sulla funzione delle decisioni costitutive.

Ricezione di informazioni provenienti da fonti accessibili al pubblico, da persone private e parti private

L'Acc ha adottato un parere sul testo proposto da EUROPOL con cui in particolare si chiede di definire regole più dettagliate relative al contenuto e alla procedura di conclusione dei *memorandum* d'intesa previsti allo scopo dall'art. 26, *par.* 2, della suddetta decisione del Consiglio 2006/960/GAI. L'Acc ha anche richiamato l'esigenza di tenere conto di aspetti quali la chiarezza delle definizioni, la legittimità del trattamento dei dati trasmessi da parti private, l'attribuzione delle responsabilità e il diritto applicabile.

Check the web

Al fine di comprendere meglio la decisione costitutiva e le modalità di integrazione del progetto *"Check the web"* (controlla la rete) nel regime giuridico per gli archivi di lavoro nella convenzione EUROPOL, nonché nella decisione del Consiglio sull'EUROPOL, il gruppo di lavoro sulle decisioni costitutive ha visitato l'EUROPOL in data 15 settembre 2009. Una relazione sulle discussioni svoltesi durante la riunione e i relativi risultati è stata presentata all'Acc, unitamente a una proposta di modifica della decisione costitutiva relativa a questo archivio.

L'Acc è stata informata sui recenti sviluppi relativi al progetto SIENA, in particolare circa l'attuazione dei requisiti in materia di protezione dei dati nella prima fase di attuazione del nuovo sistema di messaggistica. La gran parte dei requisiti di protezione dei dati richiesti dall'Acc ha trovato piena attuazione. L'Acc continuerà a seguire da vicino lo sviluppo di SIENA.

Anche nel 2009 è stata organizzata una riunione con le autorità di protezione dei dati di Paesi terzi e degli organismi con cui l'EUROPOL ha stabilito accordi operativi. All'incontro erano presenti le autorità di protezione di Norvegia, Svizzera, Croazia ed i responsabili di protezione dati di EUROJUST ed INTERPOL. L'occasione ha offerto il modo di scambiare esperienze sugli aspetti della supervisione, anche se le informazioni fornite dirette a valutare il funzionamento dell'accordo in concreto sono risultate piuttosto scarse.

Attività del Comitato ricorsi

Il Comitato ricorsi ha definito un caso riguardante la richiesta dell'interessato di accesso e verifica dei propri dati.

Le attività dell'Acc, inclusi i pareri adottati e le iniziative svolte, sono disponibili anche

in italiano sul sito dell'Acc all'indirizzo *http://europoljsb.consilium.europa.eu/documents.*

Schengen: l'attività dell'Autorità di controllo comune e la Valutazione Schengen dell'Italia

Per quanto concerne i lavori dell'Acc Schengen il perdurare dei ritardi per l'entrata in funzione del SIS II (*cfr. Relazione 2008*, p. 252) ha consentito all'Acc di continuare a svolgere i compiti di supervisione attribuiti con ulteriori iniziative, che concernono in particolare il controllo in tutti gli Stati Schengen delle modalità di inserimento delle segnalazioni di cui all'art. 95 (mandato di arresto europeo, arresto a fini di estradizione), con completamento degli accertamenti sinora svolti sulle diverse categorie di segnalazioni previste dalla Convenzione Schengen, e con un calendario per il *follow up* degli accertamenti già svolti.

È proseguita la valutazione dei risultati delle verifiche compiute con riguardo alle segnalazioni relative agli artt. 97 e 98 della Convenzione, con l'adozione dei relativi rapporti; sono stati anche esaminati gli aspetti relativi alla cooperazione tra le autorità di protezione dati (Apd), nel caso di richieste di accesso presentate in un Paese diverso da quello che ha inserito la segnalazione nel SIS. La Convenzione prevede infatti che il diritto di accesso e gli altri diritti connessi possano essere fatti valere dall'interessato in uno qualsiasi dei Paesi Schengen. Molte situazioni come, ad esempio, quella in cui la segnalazione sia stata inserita da un Paese diverso da quello cui la persona si è rivolta, ovvero decisioni amministrative o giudiziarie relative ad una segnalazione di altro Paese, richiedono una cooperazione tra le autorità competenti e le autorità di protezione dei dati.

Si è inoltre deciso di aggiornare la *"Guida per l'esercizio del diritto d'accesso"*, predisposta diversi anni addietro. Il protrarsi dell'attesa per l'entrata in vigore del SIS II - che comporta anche la soppressione dell'Acc e la sua sostituzione con un altro sistema di supervisione e prevede l'obbligo di svolgere in tutti i Paesi campagne informative sui diritti delle persone, affidando alla Commissione il compito di definirle ed organizzarle - e la considerazione che le nuove disposizioni non saranno comunque attuate prima di almeno altri due anni, mentre nuovi Paesi sono entrati a far parte del sistema Schengen, ha indotto l'Acc ad intervenire nuovamente per garantire agli interessati le informazioni necessarie per esercitare i diritti riconosciuti dalla Convenzione. L'attività di aggiornamento è stata

completata e la *"Guida per l'esercizio del diritto d'accesso"*, attualmente disponibile sul sito provvisorio dell'Acc Schengen, è raggiungibile attraverso un *link* posto sulla *home page* del sito del Garante, che contiene anche le informazioni necessarie per l'esercizio del diritto in Italia. Quanto alla campagna informativa, la Commissione già da tempo ha predisposto i modelli per la stampa di opuscoli e *poster* plurilingue, anche se le attività sono per il momento in una fase di stallo.

L'Acc ha continuato a seguire gli aspetti legati alla migrazione dei dati dal SIS al SIS II, e, in previsione dello scenario futuro della supervisione e controllo (che passerà dall'Acc all'EDPS, di concerto con le autorità di protezione dati), il Garante europeo per la protezione dei dati viene invitato a partecipare alle riunioni quando questi aspetti sono all'ordine del giorno.

In relazione all'azione comune lanciata per verificare in ciascuno dei Paesi partecipanti la regolarità delle segnalazioni inserite nel sistema, con riferimento all'art. 99 della Convenzione (sorveglianza discreta e controllo specifico) ed alle raccomandazioni formulate nel rapporto finale (che l'Autorità italiana ha ripreso nei provvedimenti conclusivi della parte nazionale dell'accertamento, uno dei quali riguarda le misure di sicurezza), è stato adottato un provvedimento che contiene le prescrizioni ritenute necessarie a conformare il trattamento alle disposizioni della Convenzione ed alle prescrizioni del Codice in materia di sicurezza (*cfr. par.* 7.3.)

Valutazione Schengen dell'Italia

L'Italia è stata sottoposta alla procedura di Valutazione Schengen, che riguarda anche il settore della protezione dati. Si tratta della seconda Valutazione, dopo la prima del settembre 2004. Il Gruppo di esperti in particolare ha avuto il mandato di verificare ruolo e poteri del Garante e l'esercizio da parte di questo della supervisione sui trattamenti di dati effettuati in base alla Convenzione.

Le visite presso il Garante e gli uffici del Ministero dell'interno si sono svolte nel gennaio del 2010 e gli esperti hanno espresso una valutazione globalmente positiva, pur raccomandando di migliorare alcune prassi ed intensificare le misure di sicurezza poste a tutela dei dati e dei sistemi, largamente in linea con le prescrizioni del Garante cui si è accennato sopra.

Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune

L'Acc ha concentrato gran parte dei suoi lavori sulla proposta di decisione volta a sostituire l'attuale base legale con uno strumento dell'Unione. Dopo un primo parere nel mese di marzo, il testo è stato modificato accogliendo le osservazioni formulate dall'Acc. Successivamente, però, il servizio giuridico del Consiglio ha chiesto di modificare il testo, che conservava alle autorità nazionali di protezione dei dati riunite in una autorità comune di controllo la supervisione sulla liceità dei trattamenti dei dati svolti nel SID (Sistema informativo doganale), in modo da introdurre una forma di supervisione centrata sul Garante europeo, del tipo di quella oggi realizzata in EURODAC.

Al riguardo, una lettera a firma del Presidente dell'Acc, dando atto del favore con cui la gran parte delle osservazioni formulate nel parere sono state accolte dal gruppo del Consiglio che discute la proposta di decisione, ha ribadito l'importanza di mantenere la forma "comune" del controllo, offrendo di articolare sul punto, laddove opportuno nel corso dei lavori. Successivamente si è giunti all'adozione di un secondo parere, limitato agli aspetti della supervisione.

Il testo finale del provvedimento prevede la forma collegiale di supervisione, ma l'art. 25 nella sua forma definitiva è scritto in modo non del tutto chiaro. La decisione è stata finalmente adottata (Decisione 2009/917/GAI del Consiglio del 30 novembre 2009) ed entrerà in vigore il 27 maggio 2011.

Inoltre l'Acc, sulla scorta dei positivi risultati della sperimentazione intrapresa (*cfr. Relazione 2008*, p. 251) ha esteso l'attività di verifica a tutti i Paesi che applicano la Convenzione, utilizzando un questionario per l'autovalutazione. Le domande si basano su *standard* internazionali e riguardano principalmente misure di sicurezza fisiche e logiche esistenti e formazione del personale.

Supervision EURODAC

La supervisione sul sistema EURODAC, attribuita come coordinamento al Garante europeo (Gepd), è proseguita con conclusione della seconda ispezione comune, basata in particolare sulla verifica delle modalità attraverso le quali viene resa l'informativa all'interessato (richiedente asilo) e sui sistemi usati per accertare il requisito dell'età (solo ultra quattordicenni) ai fini dell' acquisizione delle impronte digitali per l'inserimento nella base di dati europea.

Nella riunione di giugno è stato adottato il rapporto relativo a tale supervisione coordinata. Il documento presenta i risultati dell'attività di verifica svolta e propone alcune raccomandazioni sulle proposte di modifica delle disposizioni europee che regolano il funzionamento di EURODAC e la cooperazione ai fini dell'esame della domanda di asilo (Regolamento Dublino), raccomandazioni che sono anche destinate ad essere utilizzate a livello nazionale.

La versione finale del documento, solo in inglese, è stata resa disponibile per una diffusione sia in ambito Unione sia nazionale. Un sommario del rapporto redatto è disponibile nelle diverse lingue.

Al riguardo è da rilevare che la "eguale" partecipazione delle autorità di protezione dei dati richiederebbe un adeguato regime linguistico e la traduzione nelle diverse lingue almeno dei principali documenti - in particolare di quelli provenienti dal gruppo di lavoro di EURODAC - per la circolazione all'interno dei diversi Paesi. Attualmente la lingua di lavoro è solo l'inglese, anche per la redazione dei documenti, differentemente da quanto avviene per i lavori delle Autorità comuni di controllo. Il Garante europeo al riguardo fa riferimento al costo da sostenere, ma tale stato di cose potrebbe incidere sulla funzionalità del meccanismo di supervisione, da assicurare su base collegiale.

Altro tema approfondito nel periodo considerato ha riguardato il funzionamento della rete di comunicazione utilizzata nell'ambito della procedura di asilo (*DubliNet*): sulla base del lavoro svolto in modo coordinato nei vari Paesi è stato redatto un rapporto che presenta lo stato dei fatti e formula alcune raccomandazioni.

Il rapporto suggerisce la necessità di utilizzare *DubliNet* in modo sistematico per gli scambi di informazioni e le comunicazioni che avvengono tra gli uffici "Dublino", di dettare regole complementari a livello nazionale sull'uso del sistema (manuali d'uso, guida alle migliori prassi). Raccomanda infine, rivolgendosi in particolare alla Commissione, di dettare regole chiare ed armonizzate per quanto concerne la cancellazione dei dati una volta che la finalità dello scambio sia stata ottenuta. Anche questo documento, una volta formalmente adottato, sarà distribuito alle delegazioni e diffuso tra le autorità ed istituzioni competenti.

E' in corso l'attività per la redazione del rapporto di attività per gli anni 2008-2009 e per la definizione del programma di attività per il biennio 2010-2011.

20.4. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Case Handling Workshop

I due incontri semestrali previsti nell'ambito dei *Case Handling Workshop* si sono tenuti rispettivamente il 12-13 marzo a Praga ed il 22-23 ottobre a Limassol (Cipro).

Come di consueto, sono stati affrontati alcuni temi già discussi in precedenti riunioni del gruppo e, in particolare, in occasione del precedente *workshop* a Bratislava (*mass media* e *privacy*; videosorveglianza; trattamento di dati dei lavoratori compreso il tema del *whistleblowing*) nonché problematiche più generali, legate all'esercizio del diritto di accesso da parte degli interessati. Il *workshop* di Cipro, in particolare, è stato organizzato tenendo conto delle indicazioni della *Spring Conference* 2009, con la presentazione di *case studies* da discutere in sessioni parallele su alcuni argomenti dalla stessa indicati (oltre a quelli sopra ricordati, i trattamenti di dati personali effettuati attraverso la rete internet ed i trattamenti effettuati nel settore bancario e presso i sistemi di informazione creditizia).

Quanto al rapporto tra protezione dei dati e *mass media*, occorre rilevare che nella maggior parte dei Paesi europei il trattamento effettuato per finalità giornalistiche non rientra nella competenza delle autorità di protezione dati, essendo rimesso (visto il carattere costituzionale del diritto alla manifestazione del pensiero) all'autorità giudiziaria.

La sessione di Praga ha consentito all'Autorità finlandese di presentare il caso oggetto della sentenza della Corte di giustizia delle Comunità europee del 16 dicembre 2008 (*Satakunnan Markkinapörssi and Satamedia*), relativo all'inoltro via *Sms* - e a pagamento - dei dati reddituali raccolti da una società e dapprima pubblicati dalla stessa su un "quotidiano" regionale; l'Autorità ha richiamato l'attenzione sulla mancata specificazione da parte della Corte del concetto di *"trattamento effettuato per finalità giornalistiche"* che ha lasciato, nella sostanza, alla Suprema Corte amministrativa finlandese il compito di decidere se il predetto trattamento rientri o meno in tali finalità. L'autorità italiana ha sollevato il problema della pubblicazione *online* degli archivi storici di testate giornalistiche ma, forse per i motivi sopra riportati, nessuna esperienza simile alla nostra è stata segnalata.

Un tema sempre di attualità, anche guardando ai precedenti incontri, è quello della videosorveglianza. In occasione dell'incontro di Praga, il rappresentante dell'autorità federale tedesca ha rilevato come, a suo avviso, il tema possa essere oggetto di una futura revisione della Direttiva n. 95/46/CE che non lo affronta in modo specifico: la Germania ha una legge federale che disciplina il trattamento di dati effettuato per mezzo di strumento di videosorveglianza nelle aree accessibili al pubblico, ma non nel privato (nell'ambito del quale la questione è stata affrontata soprattutto attraverso la giurisprudenza e un'applicazione delle disposizioni generali in materia di protezione dei dati). In questo contesto, il periodo di conservazione delle immagini rappresenta da sempre una delle problematiche più spinose; durante l'incontro di Cipro se ne è discusso a partire dalla presentazione effettuata dall'autorità svizzera federale, relativa all'approccio complessivo alla videosorveglianza adottato nella confederazione elvetica. Dati per assodati alcuni princìpi fondamentali in materia di protezione dati (minimizzazione, proporzionalità, finalità), e sottolineata l'esigenza di un'opera di sensibilizzazione da parte delle autorità di protezione dati, l'autorità svizzera ha prospettato l'esigenza di un approccio basato sull'uso di misure tecnologiche (*blanking* selettivo delle immagini, *motion detection*, posizionamento) al fine di garantire il rispetto di tali princìpi; tuttavia, esistono innegabili divergenze rispetto alla congruità del periodo di conservazione delle immagini (un mese, una settimana), talora legate all'esistenza di specifica legislazione nazionale. Per quanto riguarda l'impiego della videosorveglianza in ambiti privati, la relazione della delegazione lituana durante l'incontro di Cipro ha offerto l'occasione per discutere del concetto di *"uso personale"*, trattando di un caso in cui l'installazione di una videocamera in un cortile interno ad un palazzo è stata ritenuta dall'autorità giudiziaria (chiamata a pronunciarsi sulla decisione impugnata dell'Apd) sottratta all'applicazione della normativa in materia di protezione dati (nonostante la visibilità di parte della proprietà di un altro inquilino dello stabile). Linee-guida in materia di videosorveglianza sono state elaborate dall'autorità olandese (con riferimento all'utilizzo da parte delle forze di polizia del proprio paese di un sistema di riconoscimento automatico delle targhe che, nato originariamente solo per le sanzioni relative al superamento dei limiti di velocità, è attualmente utilizzato anche per la repressione di

reati) e dall'autorità spagnola (riferite solo al settore privato, essendovi norme apposite per l'utilizzo di dispositivi di videosorveglianza nel settore pubblico). L'EDPS ha ricordato il proprio documento in materia, oggetto di consultazione pubblica a fine 2009, volto soprattutto a consentire al titolare del trattamento di valutare l'effettiva necessità di porre in essere e poi mantenere tali sistemi, attraverso una *"analisi prima dell'installazione"* (per verificare gli scopi, il fondamento normativo, l'opportunità/necessità dell'installazione, il rapporto costi/benefici) e un *"self audit"* costante su tali tipologie di trattamento. E' stata anche formulata la proposta di introdurre un "logo" armonizzato a livello Ue per segnalare la presenza di videocamere.

Un altro ambito significativo ha riguardato il trattamento dei dati personali sul luogo di lavoro. Al riguardo, il tema del *whistleblowing* (meccanismi dedicati per la segnalazione interna, in forma protetta, di irregolarità, soprattutto finanziarie) è stato affrontato a Praga attraverso il caso presentato dall'EDPS e relativo all'ufficio dell'OLAF (l'organismo comunitario per la lotta alle frodi); a giudizio dell'EDPS, esso troverebbe il suo unico fondamento normativo nel regolamento sul personale dell'OLAF, nel rispetto di una serie di princìpi: qualità dei dati, tempi di conservazione non eccedenti le finalità del trattamento (allo stato, le informazioni raccolte sono conservate per venti anni), diritto di accesso e di rettificazione da parte dell'interessato, informativa (con possibilità di differirla fino all'esito degli accertamenti). L'autorità portoghese ha invece descritto le linee-guida adottate in materia di accertamenti sul luogo di lavoro relativi all'uso di sostanze alcoliche o droghe da parte dei dipendenti; principio fondamentale è quello secondo cui i dati possono essere raccolti dal solo medico del lavoro e solo in caso di lavori che comportano particolari rischi per la sicurezza, anche di terzi, mentre il datore di lavoro può solo conoscere se il lavoratore sia idoneo o meno all'attività da svolgere. Va segnalato che durante l'incontro di Cipro l'autorità inglese ha presentato un caso che ha suscitato ampia eco nella stampa anglosassone, relativo ad una banca dati (in effetti una *black list*) dei lavoratori edili creata all'insaputa degli interessati; ciò ha costituito l'occasione per un confronto delle autorità sui mezzi a propria disposizione per bloccare e "sanzionare" un trattamento illecito di dati.

Sul rapporto fra protezione dei dati ed internet, la discussione nei due *workshop* ha toccato da un lato le attività di sensibilizzazione messe in atto da alcune autorità (l'autorità spagnola ha presentato la propria campagna di sensibilizzazione nelle scuole sull'uso di internet da parte dei minori) e, d'altro canto, il tema della responsabilità per la pubblicazione di dati personali su internet. Su quest'ultimo punto, l'autorità svedese ha descritto un caso relativo a forum di discussione e siti di *rating* (*ad es.*, di professori universitari), sollevando le questioni dell'eventuale responsabilità in capo al *service provider* per contenuti non propri, e del rischio di costringere gli ISP ad operare quali "censori" di libere forme di manifestazione del pensiero; un orientamento prevalente fra le autorità partecipanti riconoscerebbe la responsabilità in capo al *provider* che, pur a conoscenza di un contenuto chiaramente "illecito", non lo rimuova. Da ricordare anche i casi concernenti *Google StreetView*, sollevati dall'autorità ceca e da quella federale tedesca, sull'applicabilità e sull'opportunità della disciplina nazionale in materia di protezione dei dati (e, in tale contesto, sull'opportunità di richiedere, *ad es.*, una notificazione del trattamento); secondo l'autorità federale tedesca, la raccolta dei dati grezzi utilizzati per il servizio è effettuata sul territorio nazionale, gli stessi sono elaborati all'interno del veicolo che li raccoglie e solo successivamente trasferiti in un paese terzo, e dunque la normativa nazionale troverebbe applicazione.

Infine, durante l'incontro di Cipro sono state affrontate le tematiche relative, più in generale, all'esercizio del diritto di accesso ai dati. La discussione si è soffermata sull'interpretazione dell'art. 12, *par.* 1, lett. *a*), della Direttiva n. 95/46/CE che fa riferimento al diritto per l'interessato di ottenere informazioni su *"destinatari o categorie di destinatari cui sono comunicati i dati"*.

La nostra Autorità, partendo da due casi di studio e richiamando la recente sentenza del 7 maggio 2009 (caso *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*) - con cui la Corte di giustizia, nell'interpretare tale articolo, ha stabilito che gli Stati membri sono tenuti a prevedere il diritto di accesso alle informazioni sui destinatari o sulle categorie di destinatari dei dati nonché sul contenuto delle informazioni comunicate non solo per il presente, ma anche per il passato - ha fatto circolare un questionario

volto principalmente a comprendere come, negli altri ordinamenti, la norma sia stata recepita e attuata. Dalle risposte al questionario e dalla discussione è emersa una grande varietà di orientamenti nei diversi ordinamenti nazionali. Le diversità nell'interpretazione della norma sulla definizione di "destinatario" (che, in alcuni ordinamenti, viene riferita unicamente a soggetti terzi rispetto al titolare del trattamento, mentre in diversi altri comprende anche i soggetti che, nell'ambito della sua struttura, accedono ai dati), sui tempi di conservazione delle informazioni *"sul trattamento dei dati"* (che, per la Corte, gli Stati membri devono individuare bilanciando il diritto dell'interessato a conoscere queste informazioni e l'onere che l'obbligo di conservare tali informazioni comporta per il titolare del trattamento) e sui "contenuti" delle informazioni comunicate lasciano spazio a ulteriori discussioni. Si è deciso pertanto di proseguire la discussione anche nel prossimo *workshop*, con l'idea di predisporre un documento che, riassumendo l'esito del questionario, possa rappresentare alla *Spring Conference* del 2010 alcuni aspetti critici e alcuni suggerimenti per un più uniforme esercizio del diritto di accesso nei diversi Paesi.

Iwgdpt: il "Gruppo di Berlino"- *International Working Group on Data Protection in Telecommunication*

L'*International Working Group on Data Protection in Telecommunications* (*Iwgdpt*) nel corso del 2009 ha proseguito i suoi lavori con i due consueti incontri (12-13 marzo Sofia, 7-8 settembre Berlino). Durante la riunione di Sofia è stata approvata una raccomandazione sui rifiuti elettronici e la protezione dei dati, nella quale si invitano i legislatori nazionali, in cooperazione con le autorità di protezione dati nazionali e tutti gli operatori del settore industriale coinvolti, a stabilire misure per prevenire o limitare l'accesso non autorizzato ai dati personali contenuti nelle apparecchiature elettriche ed elettroniche destinate ad essere riciclate o eliminate. Nel testo si invitano i titolari dei trattamenti a prevenire o limitare la conservazione di dati negli strumenti e nelle apparecchiature in cui risulti difficile la rimozione di dati personali. Le misure indicate nella raccomandazione dovranno tener conto dei rischi connessi al riutilizzo e agli *standard* tecnici che assicurino la cancellazione dei dati personali.

La seconda riunione del *Iwgdpt* è stata dedicata in particolare all'approvazione di un documento sui rischi connessi al riuso degli indirizzi di posta elettronica e di informazioni simili. Le raccomandazioni sono rivolte agli *Internet Service Providers* ai quali viene

chiesto di prevedere un periodo di sospensiva di almeno tre mesi prima di riassegnare ad un altro utente lo stesso indirizzo e-mail o lo stesso numero di telefono, informandone adeguatamente gli abbonati precedenti e prevedendo una serie di misure di sicurezza per garantire la tutela delle informazioni personali contenute in un account momentaneamente dismesso. Le raccomandazioni sono rivolte anche ai datori di lavoro nella gestione degli indirizzi e-mail e dei recapiti telefonici dei propri dipendenti.

Consiglio d'Europa

Nel corso del 2009 l'Autorità italiana ha partecipato con impegno ai lavori del Comitato consultivo (T-Pd) della convenzione 108/1981 del Consiglio d'Europa, anche attraverso il contributo fornito alle attività del *Bureau*, gruppo ristretto volto ad assicurare continuità ai lavori del T-Pd.

In questo contesto è proseguita l'attività di predisposizione di un testo di raccomandazione in materia di profilazione (*v. Relazione 2008*, p. 260). Il progetto individua specifiche garanzie per i soggetti interessati con l'obiettivo di applicare le previsioni sancite dalla Convenzione 108/1981 alle caratteristiche che le attività di trattamento assumono nell'ambito del processo di profilazione. In quest'ottica, sono state promosse soluzioni volte a garantire 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) pur nel rispetto delle esigenze connesse all'uso di tecniche di profilazione, in grado di consentire la raccolta massiccia di dati e la loro aggregazione automatica in classi di appartenenza. Particolare attenzione è stata rivolta al diverso ambito di applicazione della raccomandazione rispetto alle attività di profilazione poste in essere da soggetti pubblici e da soggetti privati; sono stati individuati anche specifici obblighi nei confronti dei titolari del trattamento, soprattutto relativamente all'adozione di idonee e preventive misure di sicurezza.

Occorre anche ricordare che l'Assemblea Parlamentare del Consiglio d'Europa ha approvato il 28 settembre 2009 una raccomandazione per richiamare l'attenzione sulla necessità e l'opportunità di garantire la navigazione sicura dei minori su internet, in primo luogo attraverso il coinvolgimento di chi produce i contenuti di internet, ma anche con un'opera di sensibilizzazione e controllo da parte di tutti i soggetti pubblici e privati

coinvolti. La raccomandazione invita ad utilizzare la tecnologia per aumentare la sicurezza dei minori (filtri, dispositivi di limitazione degli accessi) attraverso il contributo del mondo industriale e delle imprese, a promuovere attività di sensibilizzazione attraverso l'azione congiunta delle aziende che operano su internet e dei governi nazionali, a mettere a punto ed applicare codici di condotta per la tutela della *privacy*, la promozione di attività commerciali appropriate per i minori e la sensibilizzazione sui contenuti nocivi e dannosi, anche attraverso centri di ascolto e *hotline*.

Con riferimento alle altre attività del T-Pd, è opportuno ricordare che nel corso del 2009 è stato conferito lo status di osservatore agli Stati Uniti ed alla *"European Privacy Association"*.

Inoltre, nell'ambito della consueta attività di coordinamento riguardo al *"Data protection day"*, il 2009 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.

OCSE - *Wpisp*

Il *Working Party on Information Security and Privacy* (*Wpisp*), ha proseguito i suoi lavori nel 2009, in modo particolare sui seguenti temi:

- il quadro tecnologico e le questioni critiche relative all'utilizzo delle *cd. "sensor-based network"*, ossia le reti di sensori utilizzati per monitorare e registrare condizioni del mondo reale (quali velocità, calore, luce, *ecc.*) per diversi scopi, quali la tutela dell'ambiente, il risparmio di energia, l'approntamento di servizi sanitari anche a distanza. Si è inoltre discusso di come migliorare gli aspetti tecnici dei dispositivi per un loro più rapido sviluppo e dell'opportunità di approfondire l'impatto economico e sociale di tali tecnologie, specie con riferimento alla sicurezza ed integrità dei dati trattati e alla *privacy* degli utenti; particolare attenzione è stata rivolta alla conservazione elettronica delle informazioni, alla trasparenza da garantire all'utente, alla individuazione dei soggetti a cui spettano i diritti in merito ai dati personali trattati;
- è proseguita la discussione in materia di *Identity Management* con l'intento di fornire ai *policy maker* un quadro di riferimento sulle sue diverse implicazioni, tenendo conto della particolare complessità e dell'ampia gamma di settori in cui tali

tecniche possono essere utilizzate. Fra gli elementi necessari per garantire fiducia da parte dei cittadini, e quindi lo sviluppo di questa tecnologia, sono stati evidenziati la necessità di implementare un approccio di *privacy by design*, la trasparenza nelle procedure di *enrolment* e nei trattamenti successivi, adeguate misure di sicurezza dei dati, nonché l'individuazione dei soggetti cui attribuire la responsabilità della gestione dei dati;

- il tema della tutela dei minori in internet è stato un altro argomento all'ordine del giorno dei lavori del *Wpisp*, con l'intento di promuovere un'analisi delle diverse politiche nazionali in materia di tutela dei minori sul *web*; nel medio-lungo periodo ciò dovrebbe condurre all'individuazione di politiche comuni e forme di cooperazione internazionale, anche attraverso lo scambio di esperienze nazionali e *best practices*;
- si è discusso, infine, della *cd. "privacy accountability"* sottolineando come tale approccio consenta di valutare in quale misura un'organizzazione che tratti dati personali garantisca trasparenza e responsabilità nei propri meccanismi di gestione delle informazioni personali. E' stata richiamata l'attenzione sulla differenza tra *responsibility* e *accountability*, intesa questa quale concetto più ampio, ancora in via di definizione, ma riferito all'idoneità complessiva a conseguire specifici obiettivi in termini di *privacy*.

Si fa presente, infine, che nel 2010 ricorre il trentesimo anniversario delle *Privacy Guidelines* dell'OCSE e che il *Wpisp* intende aggiornare le Linee-guida alla luce delle nuove sfide che la protezione dei dati dovrà affrontare.

Incontri con delegazioni estere

Nel dicembre 2009 l'Autorità italiana ha ricevuto una delegazione dell'autorità albanese per la protezione dei dati personali, vivamente interessata a conoscere la normativa italiana in materia di protezione dati e il funzionamento operativo di alcuni dipartimenti. Durante l'incontro, particolarmente proficuo per entrambe le parti, sono state poste le basi di una futura collaborazione con questa Autorità. Si sono svolti altresì incontri con funzionari esperti dei Ministeri dell'Interno della Romania (febbraio 2010) e della Turchia (marzo 2010) e sono in programma altri incontri con rappresentanti dell'Autorità di protezione dati della Repubblica moldava e di Israele, sulla base di precisi programmi comunitari.

21. LE ATTIVITÀ DI COMUNICAZIONE, STUDIO E RICERCA

21.1. LA COMUNICAZIONE DEL GARANTE: PROFILI GENERALI

Nel 2009 l'attività di informazione e comunicazione dell'Autorità ha proseguito nell'azione di sviluppo nell'opinione pubblica di una sempre maggiore consapevolezza dell'importanza fondamentale della protezione dei dati personali in una società, tecnologizzata e globale, caratterizzata da nuovi servizi di comunicazione elettronica e da sistemi sempre più evoluti e invasivi di raccolta e conservazione dei dati. Con questo obiettivo, particolare attenzione è stata rivolta ai giovani, più esposti ai rischi determinati da un uso scorretto delle loro informazioni, anche di quelle più intime e riservate.

Anche il 2009 è stato caratterizzato da una costante attività regolatoria e grande impegno è stato posto nel dare conto dei numerosi interventi assunti nei diversi settori. In particolare, sul fenomeno *social network* e la tutela dei minori su internet; la protezione delle reti di telecomunicazione e di comunicazione elettronica; il *telemarketing*; la sanità elettronica; il ricorso massiccio alla videosorveglianza; l'utilizzo di sistemi di raccolta dei dati particolarmente invasivi; il trattamento dei dati genetici e biometrici; la sicurezza delle grandi banche dati, pubbliche e private; il sistema della fiscalità; le banche e il credito al consumo; la trasparenza nella pubblica amministrazione, soprattutto *online*; la profilazione dei gusti e delle abitudini dei consumatori; il rispetto della dignità delle persone malate; il diritto di cronaca e la tutela della persona.

In tutti questi settori, l'Autorità ha cercato di fornire, oltre ad un'accurata e costante informazione, anche contributi esplicativi ed indicazioni operative per l'attuazione corretta delle norme.

I *media* hanno mantenuto una costante attenzione alle tematiche riguardanti la protezione dei dati personali e l'attività del Garante. Nel corso del 2009 il Servizio relazioni con i mezzi di informazione ha selezionato circa trentamila 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

oltre ottomilasettecento, delle quali tremilacento dedicate esclusivamente all'attività del Garante. Le prime pagine rivolte ai temi della protezione dei dati personali sono state oltre settecentocinquanta (di cui duecentodue riguardanti la sola Autorità).

Numerose sono state le interviste, gli interventi e le dichiarazioni pubblicate sulla carta stampata (duecentoquarantaquattro) e andate in onda su tv e radio nazionali e locali (novantaquattro).

21.2. I PRODOTTI INFORMATIVI

Nel corso del 2009 l'Autorità ha diffuso quarantotto comunicati stampa e quindici *Newsletter*.

La *Newsletter*, giunta al suo XI anno di pubblicazione (per un totale complessivo di trecentotrentadue numeri e di millecentocinquantaquattro notizie), favorisce un'approfondita informazione sia nazionale che internazionale ed è divenuta, oramai, un consolidato strumento di informazione sull'attività del Garante. La consultazione *online* e l'invio telematico ad un numero crescente di abbonati (istituzioni, pubbliche amministrazioni, imprese, liberi professionisti, giornalisti, privati cittadini) contribuiscono in maniera costante alla sua diffusione.

L'archivio digitale *"Il Garante e la protezione dei dati personali"*, giunto alla XIX edizione, ha visto quest'anno la sua prima realizzazione in un diverso formato, quello del *Dvd*. Il prodotto è stato completamente rinnovato nel *software*, nella grafica e nell'impostazione generale, ampliato nelle funzionalità, arricchito con nuovi elementi e con una nuova presentazione multimediale che illustra, attraverso animazioni e un linguaggio semplice e immediato, l'attività, le funzioni e l'organizzazione dell'Autorità. Nell'archivio, completamente aggiornato, le sezioni "Attività", "Normativa", "Informazione" e "Pubblicazioni" sono state rimodulate per rendere più semplice la consultazione *full text* e l'accesso ai testi della normativa nazionale e internazionale, dei provvedimenti, alla raccolta completa dei comunicati stampa e delle *Newsletter*. Il *Dvd*, oltre ad essere inviato a quanti ne fanno richiesta, viene distribuito al largo pubblico in occasione di manifestazioni nazionali, convegni, incontri, seminari che vedono la presenza e la partecipazione del Garante.

Al fine di attuare una comunicazione istituzionale rivolta direttamente ai cittadini, il Garante ha realizzato anche *dépliant* divulgativi in grado di illustrare i diversi temi connessi alla protezione dei dati personali. Ai nove pieghevoli fino ad ora pubblicati dedicati a vari argomenti si è aggiunto nel 2009 il *vademecum "Social network:attenzione agli effetti collaterali"*, curato dal Servizio relazioni con i mezzi di informazione e dedicato appunto al mondo delle comunità in rete.

Realizzato in occasione della *"Giornata europea per la protezione dei dati personali"* del 2009, il *vademecum* è stato pubblicato anche in lingua inglese e distribuito al *"Junior 8 Summit"*, il *meeting* dei giovani parallelo al G8 promosso dall'Unicef e svoltosi in Italia dal 4 al 12 luglio.

L'opuscolo è un'agile guida per aiutare sia persone alle prime armi, sia utenti più esperti, a sfruttare le potenzialità di strumenti di comunicazione tanto innovativi e potenti come le reti sociali, riducendo per quanto possibile i rischi per la vita privata e quella professionale.

Il *vademecum* - scritto con un linguaggio semplice, corredato da una grafica accattivante e realizzato in un formato delle stesse dimensioni di un *Cd*, pensato soprattutto per i giovani - ha suscitato grande interesse. Numerosi sono stati gli istituti scolastici, gli enti pubblici e gli organismi privati che hanno fatto richiesta di copie da distribuire a studenti, genitori, insegnanti, dipendenti, corsisti. E' stata avviata, inoltre, una collaborazione con Poste Italiane che ha consentito di effettuare la distribuzione di circa cinquecentomila copie dell'opuscolo sul *"Social network"* attraverso i principali uffici postali (duemilaottocento) presenti su tutto il territorio nazionale.

Il progetto di comunicazione istituzionale proseguirà con la realizzazione di un'ulteriore serie di *dépliant* relativi a diverse tematiche (scuola, lavoro, condominio).

21.3. I PRODOTTI EDITORIALI

Il notiziario bimestrale *"Garante privacy.it"* è giunto al suo VII anno di pubblicazione e al n. 37. Il bimestrale è destinato a personalità del mondo istituzionale ed imprenditoriale, caratterizzato da una comunicazione mirata ed essenziale, in grado di sottolineare

l'attività dell'Autorità nei diversi settori di intervento, con particolare attenzione anche al panorama internazionale. Ciascun numero del bimestrale apre con un editoriale che affronta argomenti di attualità, a firma di uno dei quattro componenti del Garante. E' in progetto una revisione grafica.

21.4. GLI INCONTRI INTERNAZIONALI

Nel corso del 2009 importanti incontri internazionali hanno registrato la presenza dell'Autorità italiana.

L'intero Collegio del Garante ed il segretario generale hanno partecipato all'annuale *"Conferenza di primavera delle autorità europee per la protezione dei dati personali"* (*Spring Conference*) svoltasi ad Edimburgo, dal 23 al 24 aprile. Al centro dei lavori le possibili iniziative per rafforzare e rendere ancora più effettive le garanzie poste a tutela dei cittadini europei. Il Presidente Francesco Pizzetti ha presieduto la sessione dedicata agli obiettivi che le autorità devono porsi per garantire effettivamente la protezione dei dati a livello individuale e sociale. Nell'ambito della conferenza ha, inoltre, presentato il rapporto di attività 2007-2008 del "Gruppo di lavoro europeo in materia di cooperazione giudiziaria e di polizia" (*Wppj*) e ha illustrato i risultati raggiunti e le iniziative future con attenzione agli sviluppi in materia di protezione dei dati personali nell'ambito del cosiddetto "terzo pilastro". Il Presidente Pizzetti è stato confermato per altri due anni a capo del Gruppo.

Dal 4 al 6 novembre le autorità garanti per la protezione dei dati personali di cinquanta Paesi si sono riunite a Madrid per la 31esima *"Conferenza internazionale sulla protezione dei dati personali"*. Nell'ambito della conferenza, il Presidente Pizzetti ha affrontato il tema del diritto d'autore *online* e la imprescindibile necessità di trovare il giusto equilibrio tra proprietà intellettuale, diritti delle imprese e tutela della riservatezza degli utenti. A Madrid è stata approvata, tra le altre, un'importante risoluzione in materia di *standard* internazionali contenente un primo pacchetto di regole e princìpi condivisi a livello mondiale, utile base di partenza per promuovere l'ulteriore armonizzazione delle garanzie in materia di *privacy*.

Ad Helsinky dal 4 al 7 febbraio, il Presidente Pizzetti ha preso parte ad un incontro

organizzato dall'Autorità per la protezione dati finlandese, intervenendo sul tema della cooperazione nel campo della sicurezza e della giustizia, ed ha illustrato l'organizzazione e i compiti dell'Autorità italiana.

Dall'8 al 9 maggio, invitato dalla Facoltà di Giurisprudenza ed Economia dell'Università di Wroclaw (Polonia), il Presidente Pizzetti ha partecipato alla seconda Sessione della Conferenza internazionale sulla *"Trasposizione del diritto dell'Unione europea nel sistema giuridico nazionale degli Stati membri"* (*Implementation of European Union Law to National Legal System of Member States*).

21.5. LE RELAZIONI CON IL PUBBLICO

Sin dalla sua creazione, l'Autorità si è presentata come istituzione vicina ai cittadini, attenta alla qualità dei servizi ed ai diritti della persona, in sintonia con i princìpi di trasparenza amministrativa introdotti dalla l. 7 agosto 1990, n. 241.

L'Ufficio relazioni con il pubblico è lo strumento organizzativo individuato dalla legge per l'attuazione delle funzioni di comunicazione istituzionale e contatto con i cittadini. L'evoluzione normativa, a partire dal d.lgs. 3 febbraio 1993, n. 29, fino alla legge 7 giugno 2000, n. 150, ha condotto alla compiuta definizione delle funzioni dell'Urp nella sua duplice veste di luogo di raccordo ideale per la partecipazione del cittadino all'attività dell'Amministrazione e di mezzo privilegiato funzionale alla comunicazione istituzionale con i cittadini.

Non deve inoltre essere trascurato il ruolo comunicativo determinante svolto anche verso l'interno dell'Autorità, in forza del quale le istanze della comunità vengono conosciute e accolte dall'Amministrazione secondo modalità improntate alla rapidità e all'efficienza.

L'immediatezza delle sollecitazioni consente all'Urp di avere una visione chiara e attualizzata dell'evoluzione delle problematiche legate alla protezione dei dati, che rende possibile il continuo riscontro dell'attività esplicata dall'Autorità con l'esperienza reale del cittadino.

Il personale preposto all'Ufficio ha il compito di dare piena visibilità all'attività

dell'Autorità, garantendo al cittadino sia la possibilità di partecipare e accedere alle diverse fasi procedimentali attraverso le forme di coinvolgimento espressamente regolamentate, sia il costante aggiornamento sulle tematiche di interesse dell'Autorità.

L'attività dell'Ufficio relazioni con il pubblico

L'attività dell'Urp si può ricondurre a tre grandi aree:

- semplificazione, con predisposizione di modulistica e di note tipo, nonché mediante assistenza al cittadino per l'accesso ai documenti ed alle procedure relativi agli strumenti di tutela predisposti dal Codice;
- comunicazione e gestione integrata dei rapporti con l'utenza, come la raccolta delle segnalazioni e delle istanze e la pubblicizzazione dell'attività dell'Autorità, in un rapporto di scambio continuo e circolare;
- informazione, mediante rapporto diretto e dedicato con l'utenza tramite mezzi di comunicazione ordinari, come il contatto telefonico o la posta elettronica, inclusa l'attività di assistenza alla navigazione all'interno del sito istituzionale.

L'esplicazione in tempo reale delle predette attività consente uno sviluppo dinamico degli *input* e la soddisfazione contestuale di più richieste. Il riconoscimento manifestato dagli utenti dell'Ufficio è legato innanzitutto alla celerità e completezza delle informazioni fornite, alla continuità ed alla flessibilità del servizio.

Nel corso dell'anno sono state ricevute numerose manifestazioni di gradimento, che permettono di confermare una stretta correlazione tra "qualità erogata" e "qualità percepita".

Anche nel 2009 l'interesse della pubblica opinione per le tematiche legate alla *privacy* è risultato in costante crescita. Come già rilevato in precedenza, in occasione di eventi riportati con grande risonanza dai mezzi di informazione, i cittadini sollecitano massivamente l'Urp con richieste di chiarimenti o nell'intento di rendere note opinioni, anche dissenzienti, in merito all'operato dell'Autorità.

Si richiamano in merito i numerosi interventi del Garante relativi all'attività giornalistica nei casi di cronaca propriamente delicati, riguardanti la pubblicazione di informazioni particolareggiate riguardo a minori, persone sottoposte ad abusi, malati o soggetti sottoposti a indagini giudiziarie, nonché alla vita quotidiana di personaggi pubblici.

Argomento particolarmente sentito dai cittadini continua ad essere quello delle telefonate pubblicitarie non autorizzate, dette anche telefonate indesiderate, e particolarmente apprezzati risultano essere gli interventi del Garante volti a contrastare i comportamenti illeciti posti in essere in questo settore.

Dall'analisi delle sollecitazioni ricevute, risulta che i cittadini sono interessati e sensibili in merito all'evoluzione della normativa che disciplina il *marketing,* in considerazione dell'invasività dell'attività in questione. Conseguentemente numerose sono state le perplessità e le preoccupazioni manifestate riguardo alle imminenti novità in materia di consenso preventivo per il ricevimento di messaggi a contenuto pubblicitario e di *opt-out.*

Presso l'Ufficio relazioni con il pubblico continuano a pervenire in un numero rilevante segnalazioni di cittadini che subiscono l'attività di disturbo: l'assistenza dell'Ufficio, in questi casi, si esplica attraverso l'illustrazione degli strumenti di tutela, la valutazione della documentazione con eventuale richiesta di integrazione; in breve, l'Ufficio indirizza il cittadino nella fase propedeutica all'avvio della procedura da parte del dipartimento competente.

Il ruolo fondamentale dell'Urp e l'interesse suscitato dalle problematiche legate alla *privacy* sono testimoniati dallo sviluppo crescente dell'attività: i contatti complessivamente registrati nel periodo di riferimento sono pari a trentaquattromilatrecentootto (contatti telefonici, e-mail, visitatori, fascicoli), con una evidente preferenza per i contatti a mezzo del telefono e della posta elettronica (per un totale di trentaduemilanovecentosettantacinque). A questi dati vanno aggiunti seicentotre fascicoli trattati nel corso del 2009.

In particolare, nell'ambito dell'attività di *back office,* l'Ufficio ha ricevuto diciottomilatrecentonovantanove quesiti per e-mail e posta ordinaria (di cui quattordicimilacinquecento sono stati oggetto di trattazione da parte dell'Ufficio relazioni con il pubblico).

Anche l'attività di *front office* è stata particolarmente rilevante, in considerazione del numero di contatti avvenuto attraverso il *call center* o direttamente ai numeri di telefono messi a disposizione dei cittadini (quattordicimilacinquecentosettantasei le telefonate pervenute nel 2009) e dell'intensa attività di ricevimento dei visitatori, conteggiati in circa settecentotrenta unità.

In proposito, l'analisi del profilo delle richieste inoltrate e la complessità delle problematiche dedotte denuncia una composizione eterogenea dell'utenza, costituita da cittadini, operatori economici, pubbliche amministrazioni, professionisti, consulenti, *ecc.*. Attraverso il continuo perfezionamento delle procedure interne, l'Urp risponde con adeguatezza alle aspettative dell'utenza in termini di tempestività ed efficienza.

Determinante per l'attività dell'Ufficio risulta essere la metodologia di approccio alle emergenze, che comporta il raffronto immediato con gli uffici e i dipartimenti competenti relativamente alla materia di interesse, ed il contestuale filtraggio e valutazione delle informazioni al fine di riportare tempestivamente i dati rilevanti ai massimi vertici dell'istituzione.

Tematiche d'interesse

Nel periodo esaminato si individuano alcune tematiche più ricorrenti, oggetto di attenzione da parte di cittadini e pubbliche amministrazioni.

Il *marketing* e le comunicazioni indesiderate (attraverso telefonate, fax, e-mail, *Sms*) rimangono fra gli argomenti oggetto di maggiore attenzione, mentre crescente è l'interesse per le problematiche relative al trattamento dei dati in ambito lavorativo, soprattutto in seguito all'entrata in vigore della legge 4 marzo 2009, n. 15 *"Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti"* e della legge 18 giugno 2009, n. 69 *"Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile"*, che hanno introdotto novità in merito alla trasparenza nelle amministrazioni pubbliche (cartellini identificativi; retribuzioni e *curricula* dei dirigenti; tassi di assenza e di maggiore presenza del personale).

Come facilmente prevedibile, in considerazione della diffusione dilagante di nuovi strumenti di comunicazione ed innovazione sociale, è stato registrato un marcato incremento di richieste di intervento del Garante sul trattamento dei dati personali operato nell'ambito dei *social network* (*Facebook, MySpace, ecc.*), i quali consentono l'immissione massiva di dati personali sulla rete internet verso un numero indeterminato di utenti, spesso senza adeguate possibilità di controllo e intervento a garanzia degli interessati.

I gravi abusi che si perpetrano in questi ambiti coinvolgono un numero crescente di cittadini.

Analogamente le problematiche inerenti alla videosorveglianza, anche in combinazione con altri strumenti di controllo, suscitano considerevole interesse da parte degli utenti, per di più in relazione all'implementazione e alla diffusione di nuove tecnologie, spesso utilizzate nell'ambito del controllo del lavoro dipendente. Risultano, infatti, numerose le richieste di chiarimento in merito alla liceità dell'uso della biometria in ambito lavorativo.

Non diminuisce l'attenzione nei confronti dell'esercizio dell'attività giornalistica: a prescindere dai casi più clamorosi, i cittadini sottopongono numerose richieste di chiarimento in merito al corretto esercizio del diritto di cronaca, anche in relazione all'attività dell'informazione *online*, vista come particolarmente delicata sia dal punto di vista della capillarità della diffusione, sia per la difficoltà di garanzia del diritto all'oblio in internet.

Risulta trasversale il considerevole interesse dei cittadini nei confronti del trattamento dei dati sanitari. Nei settori più diversi, dall'ambito più strettamente ospedaliero e sanitario a quello assicurativo o lavorativo, i quesiti relativi alle informazioni sulla salute sono molteplici e variegati nel contenuto.

Anche quest'anno sono numerosi i quesiti pervenuti dagli enti locali e, in particolare, da parte dei consiglieri comunali, in materia di accesso agli atti amministrativi.

Le problematiche relative al trattamento dei dati personali in ambito scolastico e universitario, come pure in ambito condominiale, vengono portate all'attenzione dell'Ufficio con costanza, sempre allo scopo di avere chiarimenti sull'applicazione della normativa al singolo caso di specie.

L'Ufficio ha inoltre registrato particolare sensibilità degli utenti per il trattamento di dati inerente il settore del credito, sia in materia bancaria, sia in relazione alle problematiche relative ai sistemi di informazione creditizia e di credito al consumo.

Come già rilevato in precedenza, è stata riscontrata una notevole affluenza del pubblico presso la sede dell'Ufficio in prossimità delle scadenze correlate agli adempimenti previsti dal Codice. In particolare, in materia di misure di sicurezza, la frequenza di utenti

con quesiti relativi alla nomina dell'amministratore di sistema si è notevolmente incrementata nella parte finale del periodo di riferimento, con l'avvicinarsi della scadenza per l'adempimento fissata, con l'ultima proroga, al 15 dicembre.

Le misure di sicurezza costituiscono comunque un argomento particolarmente interessante per gli utenti, oggetto di frequenti richieste di chiarimenti riguardanti l'attuazione delle indicazioni previste dalle norme di riferimento.

21.6. LE MANIFESTAZIONI E LE CONFERENZE

L'attività di divulgazione dell'Autorità espletata attraverso seminari, convegni ed altre iniziative, ha riscontrato nel 2009 un grande interesse da parte del pubblico.

Il 28 gennaio a Milano, presso l'Università Cattolica, si è celebrata la terza *"Giornata europea della protezione dei dati personali"*.

L'iniziativa, che dal 2007 viene celebrata in tutta Europa, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità che nei Paesi europei sono preposte alla protezione dei dati, è volta a sensibilizzare i cittadini sulla dignità, sui diritti e sulle libertà fondamentali da salvaguardare rispetto all'uso delle informazioni di carattere personale.

L'Autorità italiana ha organizzato questo terzo appuntamento in collaborazione con l'"Alta scuola in *Media* Comunicazione e Spettacolo dell'Università Cattolica di Milano", dedicandolo al fenomeno di *Facebook*, *My Space* e altri *social network*. L'Autorità ha avviato un confronto con gli studenti su uno degli aspetti cruciali che riguardano oggi l'uso della Rete.

I *social network* rappresentano straordinari strumenti di innovazione sociale, con i quali un numero crescente di persone si scambia opinioni e informazioni, ma vengono troppo spesso usati senza una completa conoscenza delle incognite che presentano e dei rischi che comportano. L'intero Collegio del Garante ha partecipato all'evento: Mauro Paissan ha svolto la relazione introduttiva; Francesco Pizzetti ha concluso i lavori; Giuseppe Chiaravalloti e Giuseppe Fortunato hanno preso parte al dibattito.

Per tale occasione il Servizio relazioni con i mezzi di informazione ha predisposto il

vademecum "Social network: attenzione agli effetti collaterali" con lo scopo di aiutare chi intende entrare in un *social network* o chi ne fa già parte ad usare in modo consapevole uno strumento così nuovo.

A Roma, dall'11 al 14 maggio, con il proprio *stand*, l'Autorità ha partecipato alla XX edizione del *Forum Pa*, la principale manifestazione fieristica e congressuale dedicata alla pubblica amministrazione, laboratorio di approfondimento di temi specifici.

Il Presidente Pizzetti - nell'ambito del ciclo di interviste curate da Stefano Rolando con personalità delle istituzioni, della politica, del mondo economico e sociale - ha affrontato il tema *"Libertà e privacy in Italia oggi"*.

Nei quattro giorni della manifestazione, in base ai dati forniti dagli organizzatori, è stato registrato un afflusso di circa trentasettemila visitatori; centoquindicimila visitatori virtuali e, come lo scorso anno, un significativo numero di cittadini ed operatori - stimato in una media giornaliera di circa seicento utenti - ha visitato lo *stand* del Garante dove era in distribuzione diverso materiale di documentazione.

Presso lo *stand* il personale dell'Autorità ha fornito risposte ai quesiti posti dai cittadini e dagli operatori.

A giugno il vicepresidente dell'Autorità Giuseppe Chiaravalloti, in qualità di relatore, ha partecipato al *"IV Forum internazionale della salute"* e ha illustrato le nuove linee-guida del Garante in merito al fascicolo sanitario elettronico e le prospettive sui futuri interventi nella sanità.

Il 22 ottobre, il Garante ha partecipato al *Forum ICT Security*, quest'anno dedicato alle nuove sfide della sicurezza informatica.

A novembre, il Presidente Pizzetti ha preso parte all'incontro annuale che *"Consumers' Forum"* organizza con le autorità indipendenti di controllo.

Intervenendo al dibattito sul tema *"Authority: tra sviluppo dei mercati e tutela del consumatore"* il Presidente ha illustrato la vasta attività ispettiva svolta dall'Autorità soffermandosi in particolare sul sistema bancario e sul trattamento dei dati delle carte di credito, un patrimonio di informazioni sui clienti particolarmente significativo.

21.7. IL SERVIZIO STUDI E DOCUMENTAZIONE

La redazione della *Relazione* annuale

Nel 2009 il Servizio studi ha coordinato la redazione della *Relazione* annuale con la preziosa collaborazione della Redazione *web*, avvalendosi di un progetto grafico impostato dal collega Maurizio Leante, prematuramente scomparso nel 2010.

Anche quest'anno l'elaborazione della *Relazione* ha costituito un'importante occasione di bilancio anche interno sull'attività svolta, sui provvedimenti più significativi adottati e sullo stato di attuazione del Codice, nonché di riflessione utile alla programmazione a medio e a lungo termine dell'attività.

La funzione di studio e di supporto giuridico

Il Servizio studi ha continuato a svolgere ricerche e approfondimenti su temi di interesse dell'Autorità, con riferimento alla normativa e alla giurisprudenza comunitaria ed internazionale, sia su impulso del Collegio, della Segreteria generale o dell'Ufficio che di propria iniziativa.

Si citano a titolo meramente esemplificativo approfondimenti in tema di bilanciamento tra libertà di espressione e diritto alla protezione dei dati personali, biometria e traffico telefonico, sul *cd.* "libro bianco" del Ministero del lavoro, della salute e delle politiche sociali nonché sui rapporti tra trasparenza e riservatezza della pubblica amministrazione.

È stato inoltre formulato un parere interno su una vicenda, oggetto di reclamo all'Autorità, relativa alla pubblicazione su un sito internet di un'ordinanza di custodia cautelare e, segnatamente, alla diffusione dei dati personali di terzi, contenuti nelle trasposizioni di stralci di intercettazioni telefoniche.

Al riguardo il Servizio studi, esaminati gli atti allo stato disponibili e supportato da consolidato e conforme orientamento giurisprudenziale nonché da autorevoli conferme dottrinali, ha ritenuto la pubblicazione integrale del provvedimento sostanzialmente conforme agli articoli 114 c.p.p., commi 1 e 2, e 329 c.p.p., ma ha manifestato dubbi sulla diffusione e sull'omessa cancellazione dei numerosi dati personali di terzi (anagrafici, di residenza e di utenza telefonica), giudicandole in contrasto con i princìpi di pertinenza e di non eccedenza rispetto alle finalità per le quali erano stati raccolti (art. 11, d. lgs. n. 196/2003).

Oggetto di approfondimento è stata altresì una questione relativa alla prestazione del consenso da parte di persone con problemi psichici, in merito alla quale non sono

emersi elementi utili a consentire ai medici ed agli psicologi di dare informazioni ai familiari dei pazienti affetti da disturbi mentali in assenza del consenso espresso degli interessati o in contrasto con la loro volontà.

Il Servizio studi ha inoltre espresso un parere su una richiesta di documentazione rivolta al Garante ai sensi dell'art. 391-*quater* ai fini delle indagini difensive ed ha svolto approfondimenti su possibili soluzioni interpretative di alcune disposizioni del Codice, come l'art. 10, commi 7 e 8, relativo all'individuazione del contributo spese nel caso in cui non risulta confermata l'esistenza di dati che riguardano l'interessato, e l'art. 5, comma 3, sul trattamento dei dati personali effettuato da persone fisiche per fini esclusivamente personali.

È stata inoltre fornito supporto giuridico all'attività istituzionale del Garante, fornendo alle strutture interessate documentazione nazionale ed internazionale o succinte osservazioni su questioni di interesse, quali le prospettive europee dopo il trattato di Lisbona, la Carta di Nizza e l'adesione dell'Ue alla Cedu nonché il *"credit scoring"* e l'*"opt-in"*.

I pareri sulle leggi regionali

Anche nel 2009 sono stati forniti elementi di valutazione per i pareri richiesti dalla Presidenza del Consiglio dei ministri, ai fini dell'eventuale impugnazione *ex* art. 127 della Costituzione, sulla conformità delle leggi regionali alla normativa nazionale sulla protezione dei dati personali, nel rispetto della sentenza n. 271/2005 della Corte costituzionale che, come noto, ha ricondotto la protezione dei dati personali alla materia dell'ordinamento civile, di competenza esclusiva dello Stato.

Al riguardo è risultata confermata la tendenza, già segnalata negli scorsi anni, di un sostanziale corretto esercizio della funzione legislativa da parte delle regioni in materia di protezione dei dati personali nonostante la natura trasversale della medesima e la connessa oggettiva difficoltà di individuare gli ambiti di rispettiva competenza tra Stato e regioni.

La preoccupazione principale nell'esaminare i testi legislativi è stata quella di evitare eventuali abbassamenti, ad opera dei legislatori regionali, del livello di garanzie assicurato dalla normativa nazionale e da quella comunitaria.

Si menziona, a titolo esemplificativo, una norma in materia di "elezioni primarie" per una competizione regionale in relazione alla quale è stato rilevato che la possibilità di individuare la scelta dell'elettore in base alla scheda della lista ritirata non avrebbe assicurato la segretezza del voto, con conseguente violazione della riservatezza della persona e quindi dei livelli di protezione garantiti dalla Costituzione e dalla disciplina sui dati sensibili contenuta dal Codice.

Profili problematici sono emersi anche con riferimento a: una norma che aveva previsto la pubblicazione di atti e provvedimenti sul bollettino ufficiale di una regione in assenza di una specifica e puntuale previsione normativa, in apparente contrasto con gli artt. 19, comma 3 e 20 del Codice; una legge in materia di sicurezza, con disposizioni sull'integrazione e la condivisione di banche dati tra la regione e gli enti locali, e sullo scambio di dati con le Forze dell'ordine; una disposizione sulle comunicazioni telematiche alle aziende sanitarie regionali priva della necessaria specificazione sulla natura delle informazioni e, pertanto, bisognosa dell'integrazione regolamentare di cui al citato art. 20.

I servizi interni di documentazione

Il Servizio studi ha, infine, continuato a curare l'aggiornamento del personale dell'Ufficio anche attraverso l'acquisizione e la messa a disposizione della documentazione normativa, giurisprudenziale e dottrinaria nazionale, comunitaria ed internazionale.

Come già segnalato lo scorso anno, al riguardo sono stati utilizzati criteri di selezione della documentazione molto ampi soprattutto in ragione della natura trasversale della materia e allo scopo di rendere un servizio utile ed efficiente.

In particolare è stato redatto un notiziario interno, il *"Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona"* denominato *"Osservatorio privacy"*, a cadenza tendenzialmente bimestrale, insieme con specifici *alert*, denominati *"Servizio studi news"*.

L'*"Osservatorio privacy"* raccoglie ampia documentazione suddivisa, oltre che in una parte di princìpi generali corrispondente alle principali materie del nostro ordinamento, nonché a specifici settori o profili di interesse, in quattro specifiche sezioni corrispondenti ad articolazioni di competenze all'interno dell'Autorità.

Il *"Servizio studi news"*, invece, contiene le novità soprattutto normative e giurispru-

denziali, rilevate se del caso tramite stampa estera, su questioni più direttamente riguardanti la protezione dei dati personali.

21.8. LA BIBLIOTECA

La Biblioteca, unità di articolazione della Segreteria generale, ha proceduto all'acquisizione sistematica delle pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati e alle tematiche correlate dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale. Il patrimonio della Biblioteca si è arricchito nel 2009 di oltre 3.000 nuovi titoli monografici (circa duemilatrecento in lingua straniera), con particolare riguardo alle pubblicazioni in lingua tedesca (circa 300 nuovi titoli pubblicati tra il 2007 e il 2009), a conferma del ruolo storico della Germania come *"patria della protezione dei dati"*.

Attualmente la Biblioteca possiede circa 8.000 monografie (circa 4.500 in lingua straniera) e 400 titoli di periodici e altri seriali.

Un aspetto specifico del programma di acquisizione è consistito nell'incremento della raccolta e della schedatura dei titoli analitici (documenti di spoglio) in materia di protezione dei dati che sono apparsi su monografie e periodici italiani e stranieri (principalmente periodici giuridici di lingua inglese): la documentazione conservata assomma a circa 3.600 titoli in lingua italiana e a circa 4.200 titoli in lingua straniera.

Nell'ambito delle iniziative concernenti l'ampliamento del patrimonio, va segnalato lo sviluppo di un settore bibliografico "istituzionale" con la raccolta tendenzialmente completa delle pubblicazioni a stampa (con priorità assegnata alle relazioni annuali) di tutte le autorità di protezioni dei dati in Europa e nel mondo.

Un forte sviluppo ha avuto il progetto di *"Digital library"* avviato nel 2008 in cooperazione con il Dipartimento delle risorse tecnologiche. Il sito *web* della Biblioteca è stato trasformato in portale moltiplicando il numero e la qualità delle risorse a disposizione degli utenti. Il portale è stato suddiviso in due aree funzionali. Nella prima area è possibile la ricerca di documenti sul catalogo *Opac online* (per un totale di oltre 40.000 *records* relativi a circa 6.600 entità bibliografiche).

L'*Opac* è stato integrato con una catalogazione elettronica provvisoria, in vista dell'aggiornamento completo del posseduto mediante l'utilizzo di una versione più avanzata del *software* di gestione bibliotecaria.

Nella seconda area si accede a un vasto catalogo di banche dati di accesso *web* e di accesso remoto con *link* diretti a documenti in *full-text*, riferimenti bibliografici e *abstract*.

Questa razionalizzazione delle risorse ha facilitato la collaborazione con la presidenza e i componenti del Collegio nell'ambito delle attività di studio e di ricerca e, al tempo stesso, ha permesso di supportare i dipartimenti nei loro diversi settori di competenza.

Nel 2009 la Biblioteca ha registrato circa 4.200 richieste di titoli in lettura da parte di utenti interni (+5% sul 2008) e circa 250 domande di accesso (+25%) con circa 1.800 richieste di titoli in lettura da parte di utenti esterni (+20%). I contatti sul catalogo *Opac* sono stati più di 7.000 (+17% sull'anno precedente).

In crescita esponenziale sono risultati gli accessi e le consultazioni delle banche dati giuridiche in rete dopo la creazione della apposita sezione nel portale internet della Biblioteca. I dati analitici disponibili si riferiscono ai due principali *database* giuridici, differenti per tipi di contenuto.

Il *database* della normativa, con cinque accessi multiutenza, ha totalizzato 4.418 connessioni nel 2008 con 29.950 documenti consultati (368 connessioni e 2.495 documenti di media mensile), per una durata totale degli accessi di 309.284 minuti (70 minuti di durata media), pari a oltre 5.154 ore.

Da gennaio a ottobre 2009, ultimo mese analizzato, le connessioni sono salite a 5.634 (+28%) e i documenti consultati a 37.966 (+26%), pari a 563 connessioni e 3.796 documenti di media mensile, con la durata degli accessi giunta a 383.245 minuti (68 minuti di durata media), pari a oltre 6.387 ore.

Il *database* di giurisprudenza e di dottrina, con cinque accessi multiutenza, e limitatamente al periodo marzo-novembre 2009 (con il periodo marzo-maggio di *trial*), ha registrato un totale di 470 sessioni e di 11.551 minuti di durata (88 minuti di durata media), pari a circa 192 ore.

In proiezione, le due banche dati giuridiche hanno totalizzato circa 7.550 accessi e oltre 8.000 ore di consultazione nell'arco del 2009.

In termini complessivi, a questa cifra vanno aggiunte circa 3.000 ore di consultazione di altre banche dati di accesso *web* o di accesso remoto da parte di utenti esterni e interni, portando il totale generale a oltre 11.000 ore (+37% sul 2008).

21.9. LE ALTRE INIZIATIVE DI COMUNICAZIONE E RICERCA

21.9.1. Il Laboratorio Privacy *Sviluppo*

Si è riferito nella *Relazione 2009*, (p. 276 e *ss.*) del *Laboratorio Privacy Sviluppo*, avviato con il favore del Collegio e coordinato dall'avv. Giuseppe Fortunato, che, accanto all'attività istituzionale dell'Autorità, si occupa dell'*"altra faccia della privacy"*: la libera costruzione della propria sfera privata e il pieno esercizio della *"sovranità su di sé"*, mirando all'estrinsecazione totale di ogni potenzialità della persona umana, secondo gli obiettivi di ciascuno liberamente determinati, dando conto in dettaglio delle collaborazioni instaurate in ambito istituzionale e con diversi organismi.

Il testo *"LA SVOLTA. Dal desiderio alla realtà"*, con il quale hanno avuto inizio i lavori del Laboratorio, arricchito nei contenuti e al tempo stesso, pur nella complessità degli argomenti, snellito nella forma, è stato argomento di oltre venti tesi di laurea e di Master già discusse e di numerose altre in preparazione. Esso è stato registrato vocalmente, grazie all'impegno dell'Unione Italiana Ciechi e Ipovedenti, presso l'apposito Istituto per il libro parlato per permettere la fruizione a ciechi e ipovedenti.

Specifici confronti sono stati effettuati presso importanti punti culturali: Fiera del Libro al Palazzo dei Congressi di Roma, Bibli, Gabi, Società Dante Alighieri, Blu di Prussia, Fiera del Libro Possibile a Polignano a Mare, "Lucca Autori", con un *tour* in scuole pugliesi e campane e al Festival internazionale di Pagani.

Sulla base di nuovi specifici Seminari di due giorni svolti presso il *Master* in Gestione delle Risorse Umane della LUMSA Università di Roma e presso il *Master* dell'Università Europea di Roma sono state effettuate ricerche *post Master* che hanno coinvolto docenti e studenti universitari.

In risposta a domande rivolte dai lettori de LA SVOLTA è stato altresì approntato un "Quesitario", a carattere aperto.

Agli incontri già svolti presso comuni, provincie e ordini professionali, si è aggiunto un nuovo incontro su *Second Life* (nella virtuale *"Piazza Torino 2 Italy"*) con appassionata partecipazione dei fruitori di tale piattaforma *web*, prevalentemente giovani.

Con la Commissione Europea è in corso una proficua collaborazione.

Le speciali metodologie interattive del *Laboratorio* hanno portato a una specifica iniziativa per il Garante durante la Giornata Europea della *Privacy*, denominata *"teatro al cinema"*, che ha visto sospendere una proiezione cinematografica per rappresentare dal vivo scenari alternativi al film, simulando interventi dell'Autorità Garante nelle vicende rappresentate.

E' in corso uno sperimentale Programma di formazione denominato *"Gli Argonauti de LA SVOLTA"*, di stimolo al protagonismo giovanile al fine di dare un contributo ai cambiamenti sociali e alla costruzione di una nuova *leadership*. In tale ambito lo speciale Premio Teatrale Nazionale LA SVOLTA è stato assegnato ad una rappresentazione teatrale ispirata al testo.

Con la partecipazione dei leader associativi si è svolto a Monte Citorio il 18 luglio 2009 l'incontro *"SOLO LA SVOLTA è LA SVOLTA"* in cui è stato approfondito il comune impegno di tutte le associazioni, evidenziando, già nel titolo, che solo una SVOLTA da spettatore a protagonista dell'essere umano è davvero LA SVOLTA sociale e istituzionale. Ciò è stato anche espresso in apposito giornale, distribuito in tempo reale durante l'incontro e relativo ad esso, intitolato: *"CIVICRAZIA: LA SVOLTA"*.

Dal punto di vista istituzionale tale messaggio ha poi visto le associazioni rapportarsi unitariamente alle istituzioni, chiedendo garanzia di trasparenza nei procedimenti di nomina, con affidamento a persone altamente competenti e idonee a garantire i diritti dei cittadini nei confronti della pubblica amministrazione.

Molteplici personalità del mondo della cultura, delle arti e dello spettacolo (le cui interviste sono state pubblicate nel sito *web* del Laboratorio) hanno contribuito, esprimendo apprezzamento e condivisione dell'iniziativa, sulla base delle specifiche

esperienze personali cui il Laboratorio ha tenuto conto per successivi approfondimenti.

Un'apposita convenzione è stata poi recentemente stipulata con il Ministero del Lavoro e delle Politiche sociali per la diffusione del messaggio LA SVOLTA nel mondo del lavoro.

Recentemente gli organismi e le associazioni impegnati nel Laboratorio hanno dato vita al sito *web www.civicrazia.org*, cui è collegata un'apposita piattaforma video *www.civicrazia.tv.*

Inoltre, nello spirito di un dibattito libero e aperto, il messaggio è diffuso sia tramite i *Social Network* (anche con l'azione congiunta del più numeroso insieme di gruppi su *Facebook* e anche con appositi Convegni in cui si sono incontrati i più importanti gruppi del *Network*) sia tramite il canale Civicrazia su *www.youtube.it.*

Tale percorso ha portato al varo di uno snello Manifesto e a far coincidere il messaggio della persona protagonista del Laboratorio con l'idea stessa del cittadino protagonista di *Civicrazia.*

Lo sviluppo di tali attività ha comportato una strutturazione territoriale con appositi Referenti in ciascuna regione i quali hanno organizzato Conferenze Programmatiche regionali nel mese di marzo (cosiddetta Primavera civicratica).

Sono stati, poi, costituiti il Comitato Nazionale Stampa Locale e il Comitato Nazionale Emittenti Televisive Locali (di cui fanno parte rispettivamente direttori di testate locali e direttori di emittenti televisive locali che condividono e sostengono tale messaggio).

L'Ufficio del Garante

III. L'Ufficio del Garante

22. La gestione amministrativa dell'Ufficio

22.1. Il bilancio, gli impegni di spesa e l'attività contrattuale

La gestione amministrativa dell'Ufficio è stata improntata al rispetto dei canoni di trasparenza delle procedure e della flessibilità ed efficienza dell'azione amministrativa.

Le risorse finanziarie sono state destinate a soddisfare le esigenze rappresentate nel documento programmatico approvato in sede di adozione del bilancio di previsione dell'esercizio e al perseguimento dei relativi obiettivi, nel rispetto delle procedure previste dalla legge e dai regolamenti che disciplinano la materia.

Nell'esercizio 2009 le entrate di competenza ammontano complessivamente a 15,3 milioni di euro, in riduzione di oltre 5,5 milioni di euro rispetto al precedente esercizio.

La voce più significativa delle entrate, pari a 13,1 milioni di euro, è rappresentata dal contributo erogato dallo Stato, che ha fatto registrare comunque una flessione significativa, pari a oltre 5 milioni di euro, corrispondente a circa il 27% rispetto alle somme assegnate nel precedente esercizio. Tale riduzione è ascrivibile ai minori stanziamenti di bilancio ed agli effetti restrittivi derivanti dalla legge finanziaria e dalle relative disposizioni attuative.

Le entrate proprie, pari a 1,5 milioni di euro, rappresentano circa il 10% del totale delle entrate accertate. Di queste, un importo pari a 0,8 milioni di euro è costituito da proventi di sanzioni pecuniarie, 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 importo fa registrare nell'esercizio un incremento più che doppio rispetto a quanto incamerato nel 2008 e in ciascuno degli anni precedenti.

Al risultato si è pervenuti anche a seguito di innovazioni riguardanti il procedimento amministrativo di acquisizione delle somme spettanti, il cui trasferimento al Garante avviene soltanto successivamente all'effettiva acquisizione all'entrata erariale.

Va doverosamente segnalato, tuttavia, che le entrate connesse all'attività ispettiva e di controllo, nonostante questo forte incremento, continuano ad assumere un valore marginale rispetto all'entità delle entrate complessive iscritte in bilancio.

Le spese ascrivibili alla competenza del 2009 sono pari a complessivi 24,5 milioni di euro, delle quali la parte più significativa, pari a circa 24,1 milioni di euro, attiene alle spese correnti per il funzionamento dell'Ufficio e per il corretto svolgimento delle attività istituzionali, mentre la restante parte, pari a 0,4 milioni di euro, riguarda le somme destinate all'acquisto di beni durevoli.

L'entità della spesa registra, rispetto al precedente esercizio, un incremento di circa 4,9 milioni di euro, al quale hanno concorso in misura significativa soprattutto fattori di natura straordinaria, anche connessi alla definizione di accordi contrattuali per la sede degli uffici, nonché l'aumento della spesa per il personale, per importi meno rilevanti.

Sotto quest'ultimo profilo, la variazione è determinata sia dal naturale adeguamento delle retribuzioni dei dipendenti, sia dai costi connessi alle nuove assunzioni perfezionate nel corso dell'anno, che hanno riguardato vari profili professionali.

L'immissione in servizio delle risorse nel 2009, infatti, è avvenuta nell'ambito della nuova pianta organica, a completamento di diverse procedure selettive poste in essere per adeguare l'assetto organizzativo dell'Ufficio ai compiti da svolgere.

Le spese di investimento durevole, ancorché di entità poco significativa, fanno registrare una riduzione rispetto al precedente esercizio.

Il perseguimento delle finalità istituzionali è avvenuto nel rispetto degli indirizzi di contenimento della spesa previsti dalle recenti leggi finanziarie e l'attività amministrativa dell'Autorità non ha subito ridimensionamenti, in quanto si è avuta la possibilità di sopperire alle minori risorse finanziarie disponibili rispetto alle effettive esigenze attraverso l'utilizzo di una parte delle economie realizzate negli anni pregressi.

La tabella allegata alla presente *Relazione* (*par.* 23, *tab.* 22) riassume sinteticamente i valori finanziari di competenza che hanno interessato la gestione dell'Autorità nell'esercizio 2009 e in quello precedente.

In particolare, sono evidenziate le risorse finanziarie complessivamente accertate,

tra cui quelle trasferite dallo Stato, nonché le somme complessivamente impegnate nel periodo di riferimento.

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 e ad un potenziamento di alcuni settori strategici dell'Autorità, anche per effetto dell'incremento dell'organico determinato dalle nuove assunzioni.

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 nello svolgimento dell'attività ispettiva (*cfr. par.* 19.2).

Tra le attività rientranti negli obiettivi programmatici dell'Autorità, una particolare attenzione ed un impegno significativo sono stati dedicati alle funzioni di documentazione, informazione e comunicazione, anche al fine di promuovere tra il pubblico i princìpi ispiratori della disciplina in materia di riservatezza dei dati personali.

In tale ottica, l'Autorità ha partecipato attivamente ad eventi e manifestazioni, anche di rilievo internazionale, per divulgare la conoscenza e promuovere idonee campagne informative sui diritti dei cittadini, di cui si riferisce nel *par.* 21.

Per quanto attiene all'attività negoziale, nel 2009 l'Ufficio ha fatto fronte alle normali esigenze di pianificazione degli acquisti per raggiunta obsolescenza di arredi ed attrezzature d'ufficio ed ha dato impulso ad un maggiore coordinamento tra i dipartimenti, anche al fine della necessaria ottimizzazione dei procedimenti di spesa.

Sul versante delle attività di manutenzione ordinaria della sede e delle attrezzature, l'obiettivo costante è stato quello di indirizzare gli interventi al contenimento dei costi, pur nel mantenimento degli *standard* di sicurezza e dei parametri di legge.

Tra le attività che hanno richiesto un impegno significativo, una particolare menzione è riservata a quelle connesse all'ampliamento della pianta organica dell'Ufficio ed alla conseguente allocazione del personale nei vari locali.

Nel 2009, inoltre, è stato dato un notevole impulso alle procedure telematiche di acquisizione di beni e servizi, in aderenza alle disposizioni che regolamentano la materia.

Ove consentito dalla natura dei beni e servizi da acquisire, infatti, l'attività negoziale è stata canalizzata verso procedure e servizi messi a disposizione da Consip S.p.A. e dal mercato elettronico della pubblica amministrazione.

Ciò ha permesso da un lato di beneficiare di un'amplia offerta, cui è possibile accedere sia attraverso ordini diretti, avvalendosi dei cataloghi telematici riguardanti numerose categorie merceologiche, sia in termini di richiesta di offerte da rivolgere alla platea dei fornitori presenti in listino; dall'altro uno snellimento del procedimento di acquisizione di beni e servizi, nel rispetto della trasparenza, dei parametri e dei vincoli di legge, con tangibili risparmi di spesa.

22.2. LE NOVITÀ LEGISLATIVE E REGOLAMENTARI E L'ORGANIZZAZIONE DELL'UFFICIO

Come indicato nella *Relazione 2008*, nel periodo considerato l'attività dell'Autorità è stata prioritariamente volta al consolidamento e potenziamento dell'organico dell'Ufficio, al fine di un migliore espletamento dei compiti istituzionali demandati al Garante.

L'Autorità, per dare attuazione all'incremento di organico dell'Ufficio nella misura di venticinque unità prevista dal comma 542, articolo unico, della legge 27 dicembre 2006, n. 296, (legge finanziaria 2007), nel 2009 ha completato un articolato programma di assunzioni finalizzato, in particolare, a incrementare le risorse professionali disponibili nei settori giuridico, informatico, della sicurezza informatica e della comunicazione elettronica.

Il permanere di difficoltà operative, seppure attenuate dall'immissione in servizio del personale reclutato, e la sproporzione, più volte segnalata dall'Autorità, tra i delicati e complessi compiti che il Codice, norme più recenti e la disciplina comunitaria demandano al Garante, e l'organico a disposizione, sono stati alla base della decisione di rimodulare la dotazione organica delle aree dirigenziale e direttiva mediante una riduzione di quattro posti dirigenziali (da 28 a 24) e un contestuale incremento, per un eguale numero di posti, dell'area direttiva (da 65 a 69).

A tale decisione, intesa ad assicurare un migliore e più equilibrato rapporto tra il numero dei dirigenti e quello dei funzionari, e che contribuisce altresì al contenimento del costo del personale, si è giunti sulla base di un'attenta ricognizione dei fabbisogni attuali e potenziali delle unità organizzative, per poter meglio adempiere ai predetti compiti.

In coerenza con tale obiettivo, l'Autorità si è determinata a disporre lo scorrimento della graduatoria di merito del concorso pubblico per la qualifica di funzionario con profilo giuridico-amministrativo, di recente concluso, per la copertura di ulteriori, complessivi, sei posti (in aggiunta ai cinque già coperti). Per la medesima finalità, agli inizi dell'anno in corso, si è deciso di attingere alla graduatoria di merito del concorso per la qualifica di impiegato operativo per un'ulteriore unità (in aggiunta agli otto posti già coperti in precedenza).

Come si dirà in seguito, sono state bandite alcune procedure selettive per reclutare figure professionali di particolare interesse per l'Autorità.

Nel periodo considerato è proseguita la riflessione sulle problematiche organizzative, in vista di una razionalizzazione e semplificazione dell'assetto esistente, ed è stata data concreta attuazione alla decisione di ridurre le unità temporanee di primo livello all'esito di una breve sperimentazione esauritasi nel corso del 2009.

22.3. IL PERSONALE E I COLLABORATORI ESTERNI

Agli inizi del 2009 sono stati completati i concorsi e le procedure selettive bandite dall'Autorità e si è proceduto all'immissione in servizio dei relativi vincitori.

Complessivamente sono stati coperti venti posti, di cui sedici di ruolo e quattro a contratto, ai quali vanno ad aggiungersi ulteriori sette posti attingendo alle graduatorie di merito dei concorsi pubblici per le qualifiche di funzionario con profilo giuridico-amministrativo e di impiegato operativo, di cui sei coperti agli inizi del 2010 e uno *in itinere.*

Si è conclusa, inoltre, la procedura selettiva per reclutare (sino) a tre giovani laureati con contratto di specializzazione a tempo determinato della durata di un anno e due dei suddetti posti sono stati coperti nel primo quadrimestre del 2010.

Nel periodo considerato è stata indetta e conclusa una procedura selettiva per reclutare un dirigente con profilo amministrativo-contabile da assumere con contratto a tempo determinato (il relativo avviso è stato pubblicato in *G.U.* - 4a serie speciale - 6 marzo 2009, n. 18). Ciò per coprire il posto di dirigente della competente unità organizzativa, rimasto vacante, acquisendo le necessarie competenze tecnico-professionali anche in vista della razionalizzazione dell'area amministrativo-contabile, secondo le linee di indirizzo già definite dal Collegio del Garante.

In considerazione delle perduranti carenze di personale, segnalate al paragrafo precedente della presente *Relazione*, agli inizi del 2010 è stata indetta, altresì, una procedura selettiva per reclutare quattro funzionari con profilo giuridico da assumere con contratto a tempo determinato (avviso pubblico in *G.U.* - 4a serie speciale - 26 febbraio 2010, n. 16).

Nel periodo di riferimento si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2009 l'Ufficio poteva contare su un organico, a diverso titolo, di centoundici unità, di cui centocinque in servizio, al quale va aggiunto un contingente di personale a contratto di quindici unità, alcune delle quali peraltro assunte per brevi periodi.

Dai suddetti dati si evidenzia che l'incremento di personale in servizio rispetto al precedente anno, al netto delle cessazioni, appare particolarmente significativo sia in valore assoluto (+17 unità), sia relativo (+16,5%).

Nel 2009 si è reso necessario ricorrere ad alcuni incarichi di collaborazione occasionali per attività di supporto ai dipartimenti amministrativi in tema di bilanci e di trattamenti pensionistici e ai componenti del Garante, ed è venuto a termine un incarico per la gestione dei flussi documentali necessari per attuare i regolamenti interni del Garante relativi ai procedimenti aventi rilevanza esterna previsti dal Codice.

L'Autorità si è avvalsa delle convenzioni Consip, conferendo in *insourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (*ad es.*, per l'attività di portineria e per compiti ausiliari).

Nel periodo considerato, è stato rinnovato, altresì, il servizio di controllo interno, oggi 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

Nel 2009 è continuata l'attività di sviluppo del sistema informativo, con la cura diretta della manutenzione e del funzionamento, e l'assistenza agli utenti, pur nel crescente coinvolgimento del Dipartimento risorse tecnologiche nei processi lavorativi dell'Autorità, specie in collaborazione con le unità organizzative dell'Ufficio dell'area giuridica.

Il personale del Dipartimento è intervenuto nelle ispezioni del competente Dipartimento attività ispettive e sanzioni, con 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. Rilevante è stata la partecipazione a gruppi di lavoro, a convegni internazionali, in collaborazione con il Servizio relazioni comunitarie e internazionali, e alle attività di divulgazione e comunicazione dell'Autorità, insieme all'attività di formazione interna su temi tecnologici e sulla sicurezza informatica, attraverso seminari svolti anche con esperti provenienti dall'Università o dall'industria.

Sviluppo del sistema informativo e dei servizi *ICT*

E' stato ultimato lo sviluppo del sistema di gestione del *workflow* documentale che, integrandosi con il sistema di protocollo dell'Ufficio, consente una più agevole trattazione informatica dei procedimenti, in base alle norme regolamentari sui procedimenti amministrativi aventi rilevanza esterna (*Regolamento.* n. 1/2007 [doc. *web* n. 1477480]).

E' stata consolidata la piattaforma di acquisizione della documentazione statistica *online* per l'Ufficio, integrata con i *database* e con i sistemi applicativi.

Di particolare rilievo anche il supporto alla digitalizzazione della Biblioteca, con la messa a disposizione sulla rete *intranet* dei *database* bibliografici *online*, il potenziamento delle risorse elettroniche e dei servizi *online* di consultazione delle principali banche dati giuridiche, tramite la predisposizione di nuove modalità di accesso *web* o di accesso remoto (*remote desktop*).

Nello stesso tempo è proseguita l'attività di manutenzione ed evoluzione del sistema di

gestione bibliotecaria per incrementare i servizi offerti all'utenza interna ed esterna, segnatamente per quanto riguarda il *reference* digitale.

E' stato attivato il collegamento al Sistema pubblico di connettività (Spc) previsto dal Codice dell'amministrazione digitale, che consente un efficiente funzionamento dei servizi *online* dell'Autorità, ed è stato predisposta la carta multiservizi dell'Ufficio, basata sulla Cns (Carta nazionale dei servizi), con finalità di firma digitale, *strong authentication* integrata con le procedure di *smart logon* per le postazioni di lavoro *Windows* e di *badge* per il rilevamento delle presenze.

Impegno per la sicurezza informatica dell'Ufficio

Anche nel 2009 non si sono verificati incidenti informatici nella rete interna e nei sistemi informativi dell'Ufficio, in particolare, nessun evento relativo alla sicurezza ha prodotto danni o disservizi.

Nessun *virus* informatico è penetrato sulla rete interna attraverso canali di rete o trasferimento da supporti, anche grazie all'installazione e alla messa in esercizio di un nuovo sistema per la gestione centralizzata dei *software* antivirus in grado di verificare lo stato degli aggiornamenti in modo continuo e automatico, nonché di segnalare al personale del Dipartimento gli eventi critici per la sicurezza, permettendo interventi tempestivi.

Né si sono verificate perdite di dati cui non sia stato possibile porre rimedio con le ordinarie procedure di *backup* e *recovery*. La disponibilità dei servizi gestiti in modalità *in house* si è stabilizzata sul 99,7%, con fermi macchina inferiori complessivamente alle ventiquattro ore nell'arco dell'anno (riferiti ai servizi *online* di notificazione telematica e al sistema di posta elettronica). Tale livello di disponibilità è ritenuto adeguato, e verrà comunque perseguito il raggiungimento di livelli di disponibilità ancora maggiori.

E' stata condotta un'attività di analisi, propedeutica alla certificazione ISO 27001 delle procedure di gestione della sicurezza delle informazioni nel perimetro dell'Ufficio, unitamente a un'attività di *gap analysis* secondo i *Common Criteria* delle applicazioni informatiche esposte su rete pubblica (registro dei trattamenti e notificazione telematica).

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento ha continuato a fornire consulenze alle unità dell'area giuridica dell'Ufficio, provvedendo all'analisi tecnica nella fase istruttoria dei procedimenti amministrativi, curando con relazioni, note informative e rapporti l'approfondimento di

argomenti a contenuto informatico-tecnologico, partecipando a incontri e riunioni di lavoro in cui sono stati affrontati profili tecnologici relativi ai diversi casi affrontati dall'Autorità.

Tra i temi esaminati si evidenziano: la protezione dei dati e la sicurezza dei *social network* e i rischi connessi alla massiva disponibilità pubblica di dati personali, mediante tecniche di *data mining*; la sicurezza dei servizi di messaggistica personale su reti cellulari (*Sms*), con particolare riferimento a scenari di attacco ai terminali mobili volti ad acquisire il controllo delle comunicazioni o delle informazioni degli utenti; la protezione dei dati personali nell'ambito della pubblicazione via internet di atti e documenti delle pubbliche amministrazioni; l'interfacciamento tra i sistemi informatici delle società sportive e quelli delle questure per le verifiche Daspo; le linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini; le misure di sicurezza per lo scambio di informazioni tra le amministrazioni dell'Ue e gli Stati membri nell'ambito del sistema europeo di visti VIS; la protezione di alcuni flussi di dati sensibili trattati dai sistemi informatici del nuovo sistema informativo sanitario; la misure di protezione dati personali per la realizzazione della "banca dati percettori" a cura dell'Inps; gli aspetti tecnici legati all'utilizzo di dati biometrici in vari contesti di autenticazione o di controllo degli accessi; l'aggiornamento del provvedimento sulla video sorveglianza; l'analisi preliminare delle problematiche di protezione dei dati personali nell'emergente paradigma del *cloud computing*.

Si segnalano inoltre i contributi all'elaborazione dei provvedimenti del Garante in tema di: conservazione dei dati di traffico da parte dei fornitori di servizi di comunicazione elettronica per finalità di accertamento dei reati, di cui si è riferito nel *par.* 14.1.; funzionalità e misure di sicurezza del sistema informativo SIS, per lo scambio di informazioni sugli *alert* Schengen fra gli Stati membri, e misure di sicurezza nello scambio di dati all'interno della rete transazionale SIRENE con gli uffici territoriali nazionali utili al reperimento di informazioni (*Provv.* 12 novembre 2009); monitoraggio degli accessi del dipendente (*Provv.* 2 aprile 2009 [doc. *web* n. 1606053]); accesso non autorizzato e misure di sicurezza in ambito di dati bancari (*Provv.* 28 maggio 2009

[doc. *web* n. 1624668]); maggiori garanzie per i contribuenti nell'accesso ai sistemi informativi della fiscalità in ambito di riscossione del credito (*Provv.* 7 ottobre 2009 [doc. *web* n. 1664231]).

Si evidenzia altresì la cooperazione con i dipartimenti giuridici nella preparazione dei provvedimenti relativi all'Anagrafe tributaria e agli enti esterni a essa collegati, di cui si è riferito nel *par.* 3.5.

Il Dipartimento ha poi collaborato con l'Urp, nelle risposte a quesiti e richieste di chiarimento in merito al provvedimento sugli amministratori di sistema, contribuendo all'aggiornamento delle *Frequently asked questions* (*Faq*) pubblicate sul sito ufficiale dell'Autorità e all'analisi delle richieste pervenute nell'ambito della consultazione pubblica avviata nell'aprile 2009, che ha portato successivamente all'approvazione del *Provvedimento* 25 giugno 2009 [doc. *web* n. 1626595] di modifica del precedente *Provvedimento* 27 novembre 2008 [doc. *web* n. 1577499]. Sul medesimo tema è stata continua l'attività di divulgazione e chiarimento, con la partecipazione a convegni, tavole rotonde ed eventi di comunicazione sul tema, a stretto contatto con pubbliche amministrazioni e rappresentanze di categorie (*cfr. par.* 14.2.).

Contributi all'attività ispettiva

Nonostante l'accresciuta mole di lavoro, anche nel 2009 il Dipartimento ha continuato la proficua collaborazione con le altre unità organizzative dell'Ufficio e, in particolare, con i dipartimenti giuridici e il Dipartimento attività ispettive e sanzioni.

In collaborazione con quest'ultimo ha partecipato ad impegnative verifiche ispettive, tra cui quelle relative al sistema informativo della fiscalità, gestito dall'Agenzia delle entrate, che costituisce una delle più rilevanti banche dati di interesse nazionale.

Analoghe attività sono state condotte anche nell'ambito della tutela della riservatezza delle comunicazioni elettroniche presso uno dei principali operatori telefonici nazionali, per verificare le misure di sicurezza per gli accessi ai sistemi di fatturazione.

Una rilevante azione ispettiva è stata svolta nei confronti di un'importante amministrazione locale, per verificare le misure minime di sicurezza previste dal Codice e in particolare la protezione dei dati personali contro il rischio di intrusione e l'azione dei programmi di cui all'art. 615-*quinquies* del c. p. (Allegato B. al Codice - Disciplinare tecnico in materia

di misure minime di sicurezza - regola n. 16)

Inoltre, nell'ambito dell'azione di *enforcement* a livello europeo, promossa dall'Ue *Working Party* Art. 29, sulla conservazione dei dati di traffico, il Dipartimento ha partecipato ad azioni ispettive, presso fornitori di servizi di comunicazione elettronica e *internet service provider*, rivolte alla verifica delle categorie di dati conservati, al rispetto dei tempi di conservazione e delle misure di sicurezza, secondo quanto previsto dalla direttiva comunitaria n. 24/2006/CE.

Ha preso parte anche agli accertamenti ispettivi riguardanti istituti di credito, verificando la struttura degli archivi, le tipologie di informazioni trattate, le procedure di accesso ai sistemi e alle applicazioni, i sistemi di autenticazione, le abilitazioni e le autorizzazioni degli utenti, le applicazioni utilizzate, le misure di sicurezza; agli accertamenti sugli operatori telefonici, nell'ambito dell'elaborazione di un *provvedimento* generale sulla profilazione dei dati personali; alle attività ispettive in materia di riscossione.

Contributi all'attività internazionale

Il Dipartimento ha altresì partecipato: all'attività internazionale nell'ambito dell'Ue *Working Party* Art. 29, dell'OECD *Working Party on Information Security and Privacy*, del Consiglio d'Europa, con studio di documenti e produzione di rapporti; ai lavori del *Technology Subgroup* nel WP Art. 29; all'azione di *enforcement* comunitaria rivolta ai fornitori di servizi di comunicazione elettronica e *internet service provider*, relativa al recepimento della direttiva europea n. 24/2006/CE sulla *data retention* di dati di traffico telefonico e telematico, con particolare riguardo alle verifiche delle categorie di dati di traffico conservati, dei periodi di conservazione e delle misure di sicurezza di tipo tecnico e organizzativo realizzate; ai lavori dell'*Expert Group*, istituito presso la Commissione europea, che entro il 2010 dovrà valutare il recepimento della direttiva da parte degli Stati membri; alle attività preparatorie della revisione del quadro normativo *ePrivacy*.

22.5. IL MONITORAGGIO DELL'EFFICACIA E DELL'EFFICIENZA E IL SUPPORTO AL CONTROLLO INTERNO

Nell'anno 2009 è stato potenziato, a cura dell'Unità raccolta dati, flussi informativi e supporto al controllo interno, il monitoraggio delle attività svolte dalle unità organizzative dell'area giuridica e dalle relazioni con il pubblico.

Le rilevazioni attengono alla ricognizione dei flussi documentali in entrata e in uscita, suddivisi per singole unità organizzative, raffrontate con le risorse umane.

Per fornire un monitoraggio costante, sia nel breve che nel lungo periodo, le rilevazioni sono state molteplici ed hanno avuto 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* sono stati corredati da grafici e note esplicative che agevolano la percezione dei fenomeni evidenziati nelle tabelle.

Nel periodo di riferimento si è altresì provveduto a modificare il procedimento di elaborazione dei grafici e delle tabelle, attraverso l'adozione di apposito programma ed una diversa organizzazione. Sono stati così raggiunti risultati più efficienti rispetto all'anno precedente.

Altri tipi di rilevazione hanno riguardato il volume di fascicoli arretrati suscettibile di riduzione, a partire dalle pratiche più risalenti.

Si tratta per lo più di istanze superate da provvedimenti generali dell'Autorità che hanno regolamentato la materia, o che non riscuotono più l'interesse da parte del mittente.

L'attività di monitoraggio di tale tipologia di fascicoli ha contribuito all'evasione in tempi relativamente ristretti di gran parte delle giacenze.

Anche grazie al prezioso contributo dell'Ufficio, un'ulteriore attività ha riguardato la classificazione dei numerosi fascicoli che non avevano trovato immediata rispondenza nello schema di classificazione in uso. Con la cautela dettata dall'impatto che simili strumenti possono avere sull'organizzazione, sono stati individuati approssimativi indicatori di efficienza-efficacia relativi al rapporto tra pratiche definite ed effettive risorse disponibili.

23. Dati statistici (*)

1. Sintesi delle principali attività dell'Autorità

SINTESI DELLE PRINCIPALI ATTIVITÀ DELL'AUTORITÀ	
Numero complessivo dei provvedimenti collegiali adottati	571
Ricorsi decisi (art. 145 del Codice)	360
Pareri a Presidenza del Consiglio dei ministri e ministeri (artt. 54 e 154 del Codice)	19
Altri provvedimenti collegiali sul trattamento dei dati personali	184
Notificazioni pervenute nell'anno 2009	1.048
Notificazioni pervenute dal 2004 al 31 dicembre 2009	17.559
Violazioni amministrative contestate	368
Sanzioni applicate con ordinanza di ingiunzione	101
Violazioni penali segnalate all'autorità giudiziaria	43
Riscontri a segnalazioni e reclami	3.480
Risposte a quesiti	503
Ricorsi (definiti) *ex* art. 152 del Codice	203
Opposizioni (definite) a provvedimenti del Garante	69
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	449
Altre richieste ai sensi dell'art. 157 del Codice	308
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	14
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	3
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	5
Risposte ad atti di sindacato ispettivo e di controllo	2
Leggi regionali esaminate	34
(di cui con rilievi ai fini dell'impugnazione *ex* art. 127 della Costituzione)	(2)
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	28
Riunioni Autorità comuni di controllo (Europol, Schengen, Dogane, Eurodac) e del *Wppj - Working Party on Police and Justice*	19
Riunioni presso organismi internazionali e *workshop*	11

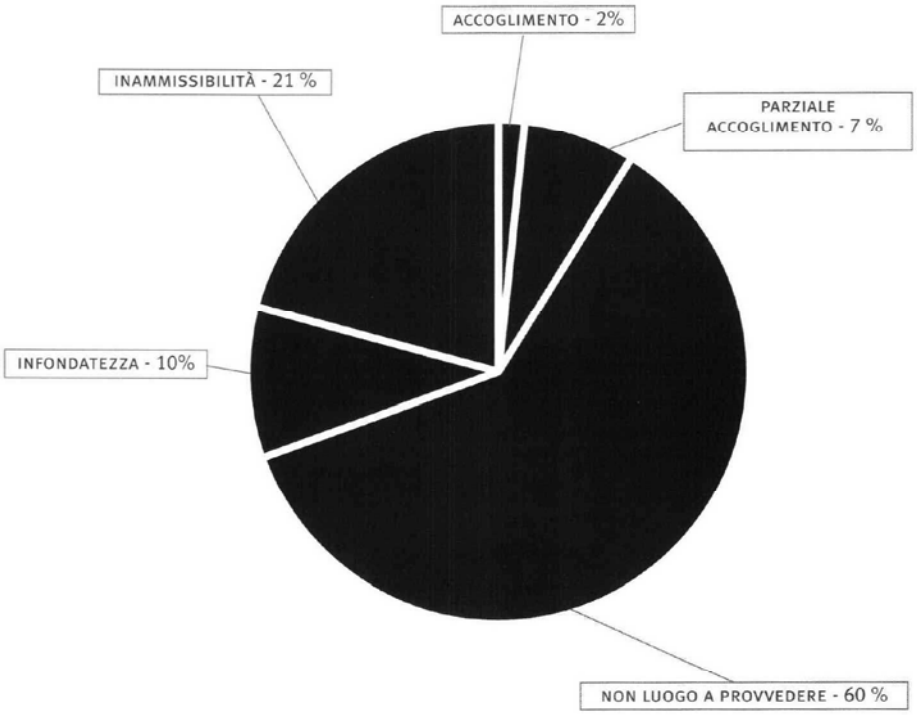
2. Altre attività

ALTRE ATTIVITÀ DELL'AUTORITÀ	
Comunicati stampa	48
Newsletter	15
Cd-rom (edizioni pubblicate)	1
Notiziario bimestrale	6
Dépliant	1
Conferenze internazionali	3

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2009. 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)

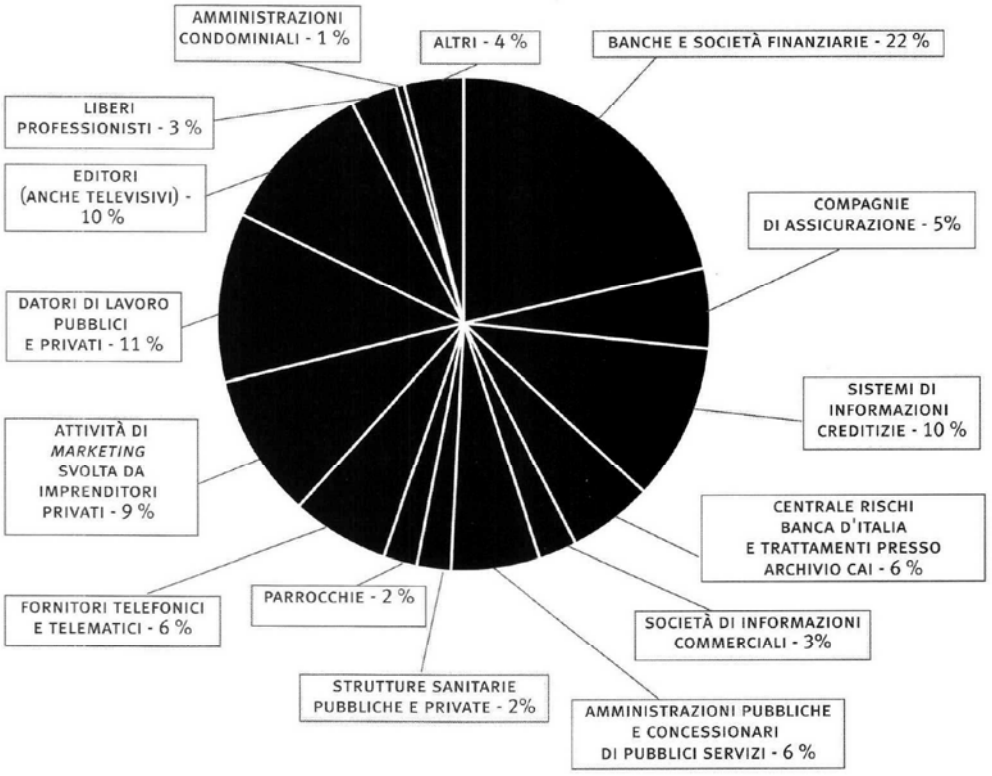
DECISIONI SU RICORSI	
TIPI DI DECISIONE (1)	NUMERO RICORSI
Accoglimento	6
Parziale accoglimento	26
Non luogo a provvedere (2)	218
Infondatezza	35
Inammissibilità	75
Totale	360



(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

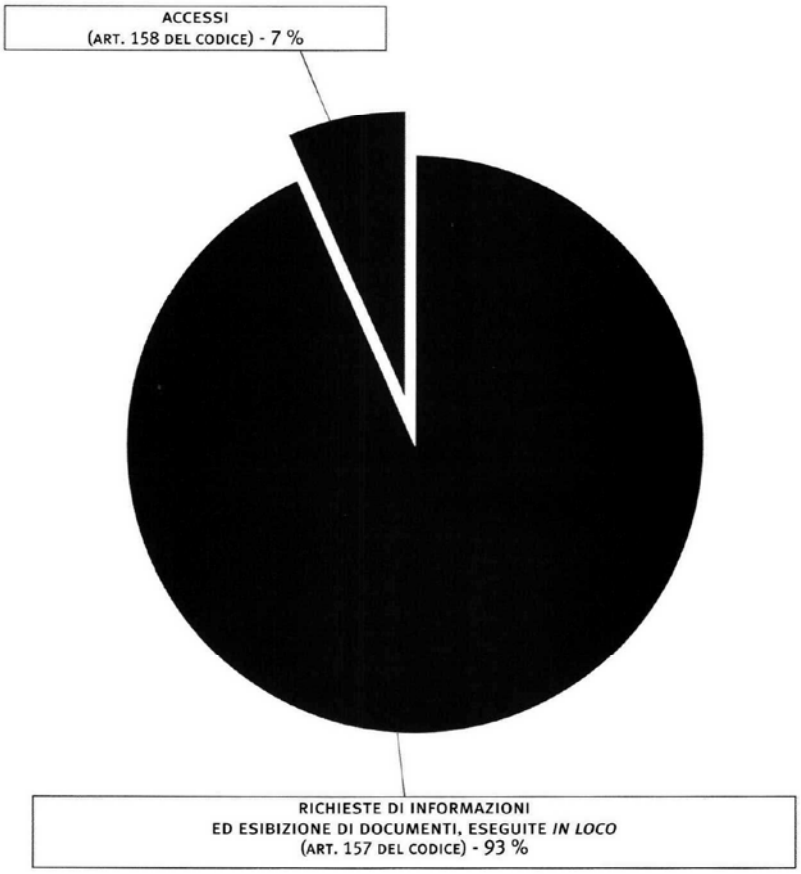
CATEGORIA DI TITOLARI	NUMERO RICORSI
Banche e società finanziarie	77
Compagnie di assicurazione	19
Sistemi di informazioni creditizie	37
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	20
Società di informazioni commerciali	9
Amministrazioni pubbliche e concessionari di pubblici servizi	21
Strutture sanitarie pubbliche e private	8
Parrocchie	8
Fornitori telefonici e telematici	23
Attività di *marketing* svolta da imprenditori privati	34
Datori di lavoro pubblici e privati	40
Editori (anche televisivi)	37
Liberi professionisti	11
Amministrazioni condominiali	2
Altri	14
Totale	**360**

4. Suddivisione dei ricorsi in relazione alla categoria di titolari del trattamento (tabella e grafico)



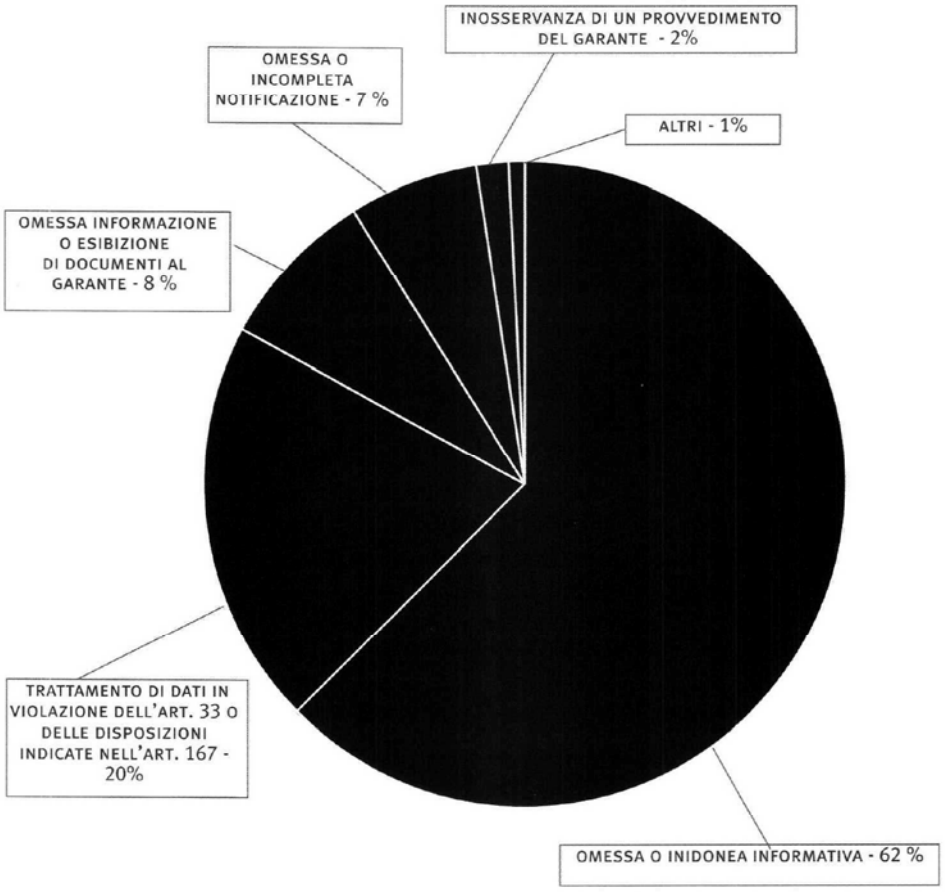
5. Accertamenti e controlli eseguiti (tabella e grafico)

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)	419
Accessi (art. 158 del Codice)	30
Totale	449



VIOLAZIONI AMMINISTRATIVE CONTESTATE	
Omessa o inidonea informativa (art. 161 del Codice)	230
Trattamento di dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	75
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	30
Omessa o incompleta notificazione (art. 163 del Codice)	24
Inosservaza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	6
Sanzioni in materia di conservazione di dati di traffico (art. 162-*bis*, del Codice) (1)	1
Più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice) (1)	1
Codice del consumo (art. 62 del codice del consumo, *d.lgs.* 206/2005) (1)	1
Totale	**368**
Somme versate a titolo di oblazione in via breve	1.572.432

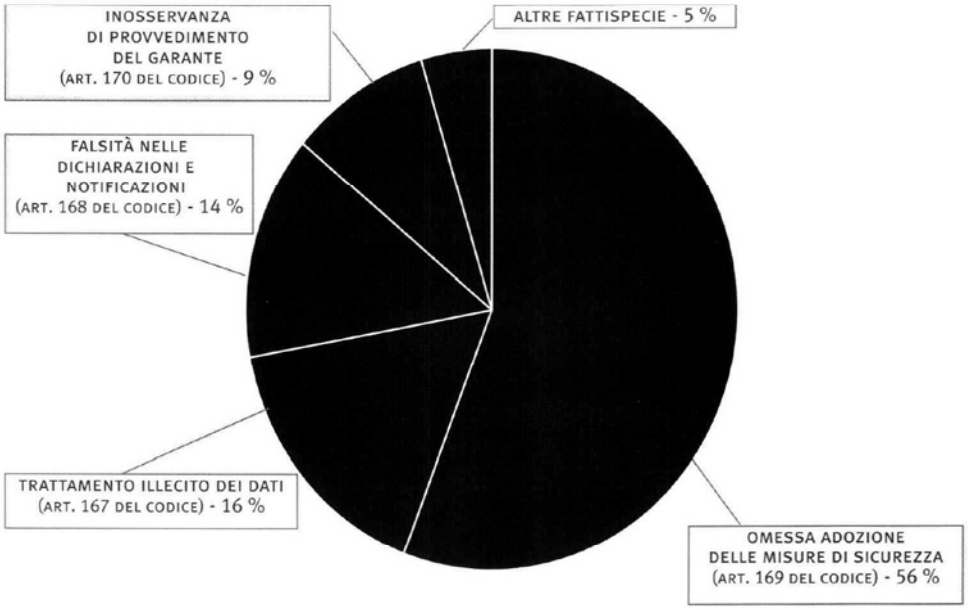
6. Violazioni amministrative contestate (tabella e grafico)



(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)	24
Trattamento illecito dei dati (art. 167 del Codice)	7
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	6
Inosservanza di provvedimento del Garante (art. 170 del Codice)	4
Altre fattispecie	2
Totale	**43**
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	**62.500**



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.	4
Formazione	2
Rapporto di lavoro pubblico	1
Protezione civile	1
Tutela della salute e attività sanitaria	5
Soggetti privati e attività produttive	1
Totale	**18**

(1) Inerenti anche ad affari pervenuti anteriormente al 2009

9. Quesiti

QUESITI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	326	503
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	16	13
Dati dei dipendenti e fascicoli personali	15	23
Giornalismo	2	1
Giustizia e accertamenti di polizia	5	12
Internet e informatizzazione	9	13
Ricerca genetica e genealogia		2
Rilevazioni biometriche	6	4
Sanità e servizi di assistenza sociale	23	49
Telefonia	3	9
Trasparenza	8	14
Tributi	3	4
Videosorveglianza	6	27

10. Segnalazioni e reclami

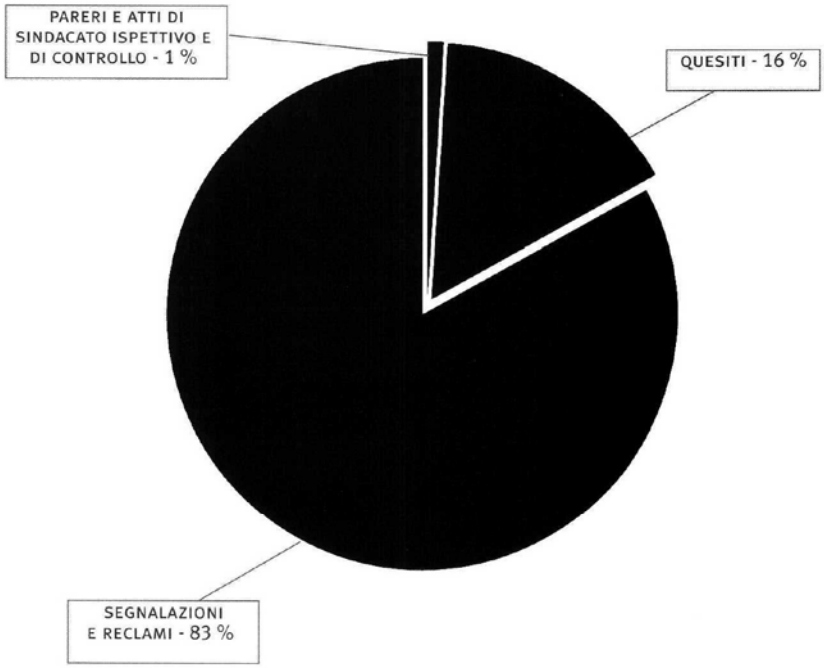
SEGNALAZIONI E RECLAMI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	3.493	3.480
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	16	23
Assicurazioni	119	111
Associazioni	46	34
Centrali rischi	246	211
Condominio	41	28
Corrispondenza	14	32
Credito	306	222
Dati dei dipendenti e fascicoli personali	47	78
Giornalismo	65	87
Giustizia e accertamenti di polizia	44	70
Imprese	138	91
Informazioni commerciali	31	14
Internet e informatizzazione	151	110
Lavoro	100	92
Marketing	271	104
Pubblicità non gradita	23	54
Recupero crediti	76	83
Rilevazioni biometriche	19	18
Sanità e servizi di assistenza sociale	41	71
Telefonia	503	445
Trasparenza	7	20
Tributi	24	58
Videosorveglianza	220	201

(1) Inerenti anche ad affari pervenuti anteriormente al 2009

11. Atti di sindacato ispettivo e controllo

ATTI DI SINDACATO ISPETTIVO E CONTROLLO	
TEMI	NUMERO
Messaggi telefonici *cd.* "*Sms*-spia"	1
Intercettazioni di comunicazioni nell'ordinamento federale Usa	1
Totale	2

12. Tipologie dei riscontri resi a interessati e richiedenti



13. Tipologie di notificazioni pervenute nel 2009

NOTIFICAZIONI - TIPOLOGIE			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	48	587	635
Modifica di una precedente notificazione	14	321	335
Notificazione della cessazione del trattamento	8	70	78
Totale	70	978	1.048

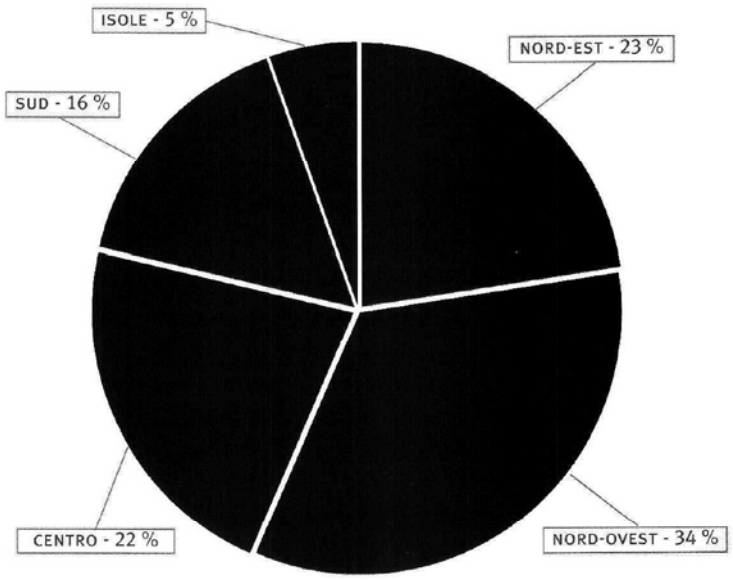
(1) Situazione alla data del 31 dicembre 2009

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL PERIODO 2004-2009			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	1.053	14.057	15.110
Modifica di una precedente notificazione	71	1.935	2.006
Notificazione della cessazione del trattamento	40	403	443
Totale	1.164	16.395	17.559

14. Tipologie di notificazioni pervenute nel periodo 2004-2009

PROVENIENZA GEOGRAFICA DELLE NOTIFICAZIONI: 2004-2009	
ITALIA	
ZONE GEOGRAFICHE	PERVENUTE
Nord- Est	3.979
Nord- Ovest	5.962
Centro	3.874
Sud	2.741
Isole	943
Totale	17.499
Da altri Paesi	60

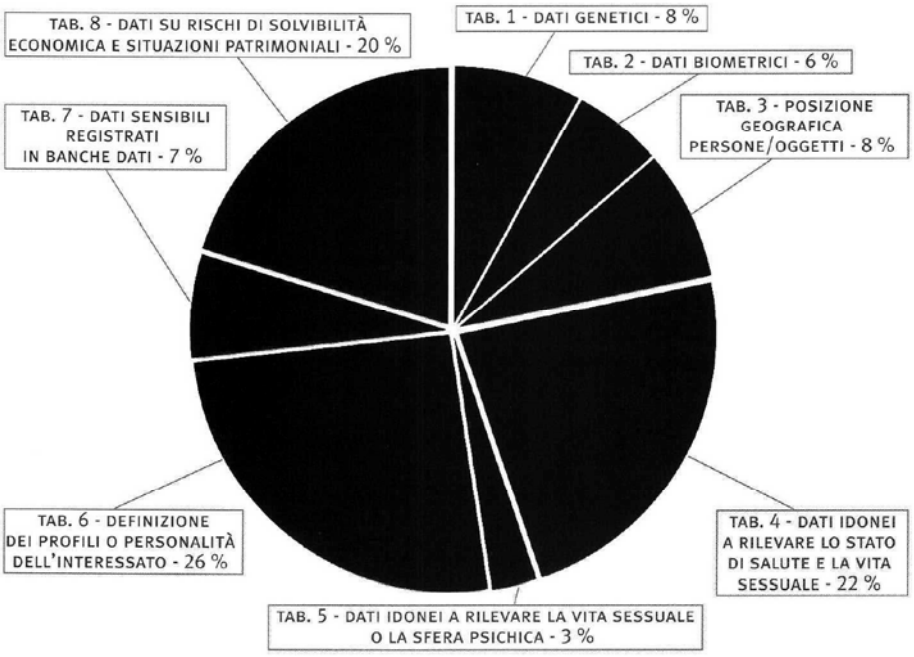
15. Provenienza geografica delle notificazioni (tabella e grafico)



(1) Situazione alla data del 31 dicembre 2009

16. Suddivisione delle notificazioni per tipologia di trattamento periodo 2004-2009 (tabella e grafico)

SUDDIVISIONE DELLE NOTIFICAZIONI PER TIPOLOGIA DI TRATTAMENTO PERIODO 2004-2009	
TABELLE DI NOTIFICAZIONE COMPILATE (1)	NUMERO
Tabella 1 - Trattamento di dati genetici	2.046
Tabella 2 - Trattamento di dati biometrici	1.478
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	2.183
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	5.810
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	716
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	6.731
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	1.689
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	5.212
Totale	25.865



(1) Situazione alla data del 31 dicembre 2009

MODALITÀ DI INOLTRO DELLE NOTIFICAZIONI PERIODO 2004-2009	
Attraverso intermediari	9.135
Direttamente a cura dei titolari	8.424
Totale	17.559

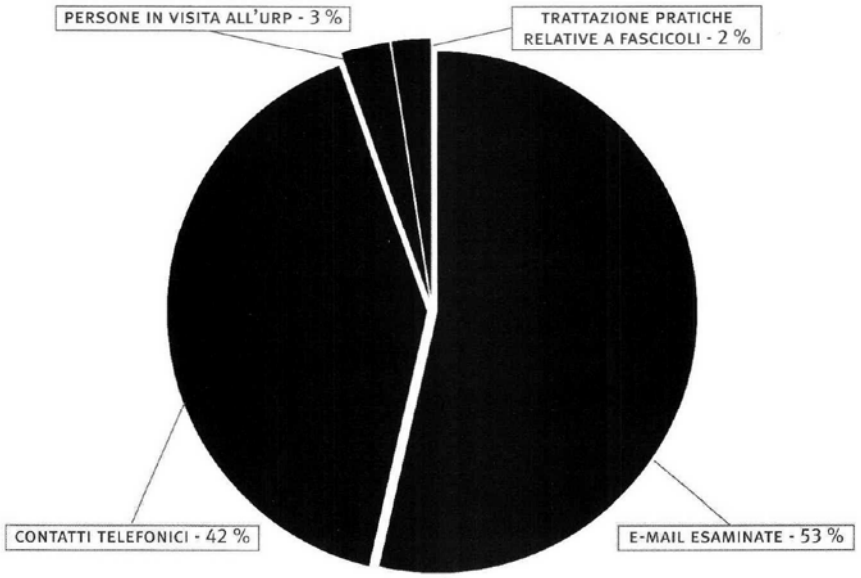
17. Modalità di inoltro delle notificazioni periodo 2004-2009

MODALITÀ DI VERSAMENTO UTILIZZATE		
TIPO MOVIMENTO	NUMERO	TOTALE EURO
Versamento mediante bollettino postale	345	51.750
Versamento mediante bonifico bancario	399	59.850
Versamento mediante carta di credito	304	45.600
Totale	1.048	157.200

18. Modalità di versamento utilizzate

UFFICIO RELAZIONI CON IL PUBBLICO			
	2008	2009	TOTALE
E-mail esaminate	19.497	18.399	37.896
Contatti telefonici	14.900	14.576	29.476
Persone in visita all'Urp	1.100	730	1.830
Trattazione pratiche relative a fascicoli	883	603	1.486
Totale	36.380	34.308	70.688

19. Ufficio relazioni con il pubblico (tabella e grafico



20. Posti previsti in organico

POSTI PREVISTI IN ORGANICO	
Segretario generale	1
Dirigenti	28
Funzionari	65
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	2	16
Funzionari	59	4	4	59
Operativi	26	3		29
Esecutivi				0
Totale	**101**	**10**	**6**	**105**
Personale a contratto				15

22. Risorse finanziarie

RISORSE FINANZIARIE						
ENTRATE ACCERTATE	ANNO 2009		ANNO 2008		DIFFERENZA	
Correnti		15.317.834,54		20.895.487,96		-5.577.653,42
di cui trasferimento dallo Stato	13.135.167,00		18.162.911,45		-5.027.744,45	
Totale entrate		**15.317.834,54**		**20.895.487,96**		**-5.577.653,42**
SPESE IMPEGNATE	ANNO 2009		ANNO 2008		DIFFERENZA	
Funzionamento		24.124.021,56	19.094.234,86			5.029.786,70
Capitale		438.755,19	570.985,77			-132.230,58
Totale spese		**24.562.776,75**	**19.665.220,63**			**4.897.556,12**

(1) Situazione alla data del 31 dicembre 2009

Documentazione

IV. Documentazione

24. Provvedimenti del Garante

Trattamento dei dati sensibili e giudiziari presso la Scuola superiore della pubblica amministrazione locale

12 febbraio 2009 [doc. *web* n. 1597595]

Giornalismo: diffusione di dati su minori vittime di violenza sessuale

16 febbraio 2009 [doc. *web* n. 1590076]

Marketing via e-mail: comunicazioni promozionali solo con il consenso preventivo dell'interessato

19 febbraio 2009 [doc. *web* n. 1597146]

19 febbraio 2009 [doc. *web* n. 1597151]

19 febbraio 2009 [doc. *web* n. 1597163]

Condominio: limiti alle comunicazioni di dati relativi alla Tarsu da parte dell'amministratore

19 febbraio 2009 [doc. *web* n. 1601650]

Videosorveglianza in un condominio

19 febbraio 2009 [doc. *web* n. 1601674]

Prescrizioni per la videosorveglianza in un supermercato

26 febbraio 2009 [doc. *web* n. 1601522]

Illecito trattamento di dati da parte di un centro tricologico

26 febbraio 2009 [doc. *web* n. 1601558]

Marketing via fax: comunicazioni promozionali solo con il consenso preventivo dell'interessato

26 febbraio 2009 [doc. *web* n. 1601475]

26 febbraio 2009 [doc. *web* n. 1601506]

Prescrizioni per il Sistema informativo delle operazioni degli enti pubblici (Siope)

26 febbraio 2009 [doc. *web* n. 1605504]

Avvio di consultazione pubblica in tema di "Linee-guida in tema di fascicolo sanitario elettronico e di dossier sanitario"

5 marzo 2009 [doc. *web* n. 1598313]

Biglietti *online*: il consenso all'uso dei dati non deve mai essere condizionato

5 marzo 2009 [doc. *web* n. 1615731]

Prescrizioni per la videosorveglianza presso i siti di interesse culturale maggiormente esposti alla minaccia terroristica

12 marzo 2009 [doc. *web* n. 1605521]

Aggiornamento del Programma statistico nazionale 2009/2010

12 marzo 2009 [doc. *web* n. 1605530]

Prescrizioni ai titolari di banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 a seguito della deroga introdotta dall'art. 44 d.l. n. 207/2008

12 marzo 2009 [doc. *web* n. 1598808]

Anagrafe tributaria: prescrizioni su sicurezza e accessi - proroga dei termini

26 marzo 2009 [doc. *web* n. 1605576]

Preiscrizioni universitarie per l'anno accademico 2009/2010

26 marzo 2009 [doc. *web* n. 1606014]

Diritto di ispezione al libro soci nelle società per azioni

26 marzo 2009 [doc. *web* n. 1606023]

Onlus: uso dei dati degli iscritti a scopo propagandistico-elettorale

26 marzo e 2 aprile 2009 [doc. *web* n. 1606059]

Giornalismo: diffusione di dati di interesse clinico e dignità della persona

2 aprile 2009 [doc. *web* n. 1605603]

Giornalismo: diffusione di dati su vittime di violenza sessuale

2 aprile 2009 [doc. *web* n. 1605613]

Lavoro privato: comunicazione di dati idonei a rivelare le condizioni di salute del dipendente

2 aprile 2009 [doc. *web* n.1605667]

Lavoro privato: monitoraggio degli accessi internet del dipendente

2 aprile 2009 [doc. *web* n. 1606053]

Trattamento di dati biometrici per finalità di autenticazione di accesso a particolari aree aziendali

8 aprile 2009 [doc. *web* n. 1610018]

Prescrizioni in materia di operazioni di fusione e scissione fra società

8 aprile 2009 [doc. *web* n. 1609999]

Giornalismo: diffusione di dati su vittime di violenza sessuale

8 aprile 2009 [doc. *web* n. 1610028]

Controllo delle esenzioni sanitarie e trattamento dei dati personali

8 aprile 2009 [doc. *web* n. 1611955]

Archivi storici *online* dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni

15 gennaio 2009 [doc. *web* n. 1589209]

8 aprile 2009 [doc. *web* n. 1617673]

22 maggio 2009 [doc. *web* n. 1635938]

28 maggio 2009 [doc. *web* n. 1635910]

25 giugno 2009 [doc. *web* n. 1635966]

23 luglio 2009 [doc. *web* n. 1639172]

19 novembre 2009 [doc. *web* n. 1689109]

22 dicembre 2009 [doc. *web* n. 1695208]

Autorizzazione per uno studio epidemiologico di pazienti oncologici, senza consenso informato

16 aprile 2009 [doc. *web* n. 1611936]

Stadio: controlli di sicurezza e rispetto della *privacy*

16 aprile 2009 [doc. *web* n. 1615614]

Amministratori di sistema: avvio di una consultazione pubblica

21 aprile 2009 [doc. *web* n. 1611986]

Graduatorie *online* e trattamento di dati idonei a rivelare lo stato di salute

21 aprile 2009 [doc. *web* n. 1616870]

Lo scontrino fiscale "parlante" per l'acquisto di farmaci

29 aprile 2009 [doc. *web* n. 1611565]

Conservazione dei dati di traffico: proroga dei termini

29 aprile 2009 [doc. *web* n. 1612508]

Servizi postali: Poste italiane resta titolare del trattamento anche in caso di appalto

29 aprile 2009 [doc. *web* n. 1617709]

Sanità: sistema informativo per le dipendenze e *privacy*

6 maggio 2009 [doc. *web* n. 1615306]

Giornalismo: uso di immagini tratte dai *social network*

6 maggio 2009 [doc. *web* n. 1615317]

6 maggio 2009 [doc. *web* n. 1615339]

Sistema informativo per la salute mentale: trattamento di dati sanitari e sensibili

6 maggio 2009 [doc. *web* n. 1616893]

Esonero dall'informativa per l'Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito (Ancic)

14 maggio 2009 [doc. *web* n. 1616828]

Prove di ammissione ai corsi di laurea ad accesso programmato per l'anno accademico 2009/2010

14 maggio 2009 [doc. *web* n. 1617715]

Divieto all'invio di comunicazioni promozionali via posta elettronica senza consenso preventivo

22 maggio 2009 [doc. *web* n. 1621346]

22 maggio 2009 [doc. *web* n. 1621355]

Divieto all'invio di comunicazioni promozionali via telefax senza consenso preventivo

22 maggio 2009 [doc. *web* n. 1621185]

22 maggio 2009 [doc. *web* n. 1621340]

22 maggio 2009 [doc. *web* n. 1621364]

Sospensione, nelle aree interessate dagli eventi sismici in Abruzzo, dei termini per gli adempimenti dei provvedimenti del Garante

28 maggio 2009 [doc. *web* n. 1620165]

Dati bancari: accesso non autorizzato e misure di sicurezza

28 maggio 2009 [doc. *web* n. 1624668]

Accordo Italia-Usa: cooperazione per la prevenzione e lotta alle forme gravi di criminalità

28 maggio 2009 [doc. *web* n. 1624697]

Dati bancari: illecita comunicazione

28 maggio 2009 [doc. *web* n. 1624734]

Illecita comunicazione di dati personali relativi alla situazione debitoria

28 maggio 2009 [doc. *web* n. 1624760]

Fidelity card: prescrizioni su trattamento eccedente di dati personali e informativa al cliente

28 maggio 2009 [doc. *web* n. 1625257]

Adempimenti *privacy* semplificati per il Servizio nazionale di protezione civile in Abruzzo

4 giugno 2009 [doc. *web* n. 1621162]

Videosorveglianza e biometria per esigenze di sicurezza: impiego non conforme

4 giugno 2009 [doc. *web* n. 1629975]

Servizi turistici e trattamento dei dati personali

4 giugno 2009 [doc. *web* n. 1630006]

Accesso dell'interessato ai dati personali contenuti in perizie medico-legali

4 giugno 2009 [doc. *web* n. 1630066]

17 settembre 2009 [doc. *web* n. 1656621]

17 settembre 2009 [doc. *web* n. 1656632]

Dati sensibili e giudiziari del personale militare

12 giugno 2009 [doc. *web* n. 1630403]

Perentorietà del termine per la regolarizzazione dei ricorsi

12 giugno 2009 [doc. *web* n. 1633383]

Trattamenti dei dati per fini esclusivamente personali

12 giugno 2009 [doc. *web* n. 1633575]

12 giugno 2009 [doc. *web* n. 1634343]

22 dicembre 2009 [doc. *web* n. 1695177]

Biometria e rilevamento della presenza del personale aeroportuale

12 giugno 2009 [doc. *web* n. 1635731]

Fotografie riprese all'interno di luogo di dimora privata: divieto di diffusione

18 giugno 2009 [doc. *web* n. 1623306]

Sportello unico per le attività produttive

18 giugno 2009 [doc. *web* n. 1630376]

Passaporto: aggiornamenti grafici e tecnici

18 giugno 2009 [doc. *web* n. 1630387]

Rilascio del passaporto elettronico

18 giugno 2009 [doc. *web* n. 1630422]

Dati bancari: accesso non autorizzato e misure di sicurezza

18 giugno 2009 [doc. *web* n. 1635720]

Lavoro: buste paga e dati che rivelano lo stato di salute del dipendente

18 giugno 2009 [doc. *web* n. 1640331]

Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento

25 giugno 2009 [doc. *web* n. 1626595]

Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione

25 giugno 2009 [doc. *web* n. 1629107]

Linee-guida in tema di referti *online*

25 giugno 2009 [doc. *web* n. 1630271]

Lavoro pubblico: diffusione *online* di dati sullo stato di salute di un dipendente

25 giugno 2009 [doc. *web* n. 1640102]

Anagrafe tributaria: proroga per i collegamenti tramite *web service* (Inps, Inpdap, Avcp e Enpals)

2 luglio 2009 [doc. *web* n. 1640373]

Ordini per telefono: si può richiedere copia della registrazione

8 luglio 2009 [doc. *web* n. 1638561]

Linee-guida in tema di fascicolo sanitario elettronico (Fse) e di *dossier* sanitario

16 luglio 2009 [doc. *web* n. 1634116]

Inammissibilità del ricorso nei confronti del Senato della Repubblica

16 luglio 2009 [doc. *web* n. 1638472]

Pubblica amministrazione: dirigenza e assenze e presenze del personale

16 luglio 2009 [doc. *web* n. 1639950]

Anagrafe tributaria: ripristino temporaneo dei collegamenti esterni (Inps)

17 luglio 2009 [doc. *web* n. 1639318]

Libertà d'informazione e protezione dei dati personali

23 luglio 2009 [doc. *web* n. 1639507]

Trattamenti dei dati per fini esclusivamente personali

23 luglio 2009 [doc. *web* n. 1639978]

Dati bancari: accesso non autorizzato e misure di sicurezza

23 luglio 2009 [doc. *web* n. 1640294]

Anagrafe tributaria: ripristino temporaneo dei collegamenti esterni (Agea e camere di commercio)

23 luglio 2009 [doc. *web* n. 1640317]

Anagrafe tributaria: proroga per la disattivazione delle utenze Siatel

23 luglio 2009 [doc. *web* n. 1640349]

Trasporto aereo: programmi di fidelizzazione e informativa

23 luglio 2009 [doc. *web* n. 1640398]

Scuola: videosorveglianza contro atti vandalici

4 settembre 2009 [doc. *web* n. 1651744]

Dati più aggiornati nel Ced del Viminale

10 settembre 2009 [doc. *web* n. 1658464]

Misure relative alle comunicazioni fra intermediari finanziari appartenenti al medesimo gruppo in materia di antiriciclaggio

10 settembre 2009 [doc. *web* n. 1664492]

Privacy garantita per l'Anagrafe dei fondi sanitari

17 settembre 2009 [doc. *web* n. 1655693]

Vigilanza più "vigilata" negli aeroporti

17 settembre 2009 [doc. *web* n. 1655708]

Cartella clinica del defunto e diritti del convivente

17 settembre 2009 [doc. *web* n. 1656642]

Trasparenza della p.a. e dati sulla salute *online*

17 settembre 2009 [doc. *web* n. 1658335]

Anagrafe tributaria: proroga degli adempimenti

24 settembre 2009 [doc. *web* n. 1657692]

Aggiornamento 2009/2010 del Programma statistico nazionale: prospetti informativi

24 settembre 2009 [doc. *web* n. 1657731]

Lavoro: anonimato per la diagnosi Hiv

24 settembre 2009 [doc. *web* n. 1658058]

2 ottobre 2009 [doc. *web* n. 1658119]

Strumenti informatici aziendali e *privacy* del dipendente

2 ottobre 2009 [doc. *web* n. 1665170]

Patronati sindacali e trattamento di dati riguardanti i lavoratori

2 ottobre 2009 [doc. *web* n. 1666101]

Regioni e riqualificazione professionale: sì del Garante *privacy* alla consultazione della banca dati dell'Inps

7 ottobre 2009 [doc. *web* n. 1658413]

Riscossione: maggiori garanzie per i contribuenti

7 ottobre 2009 [doc. *web* n. 1664231]

No ai dati sanitari sul sito del Comune

7 ottobre 2009 [doc. *web* n. 1664456]

Imprese: vietato l'uso della biometria per la rilevazione delle presenze e dei tempi di lavoro

15 ottobre 2009 [doc. *web* n. 1664257]

Stop a fax selvaggio

21 ottobre 2009 [doc. *web* n. 1667012]

Dati di traffico tlc e internet: no a conservazione illimitata

21 ottobre 2009 [doc. *web* n. 1683093]

19 novembre 2009 [doc. *web* n. 1695368]

19 novembre 2009 [doc. *web* n. 1695393]

Ministero della difesa: prescrizioni per il trattamento di dati idonei a rivelare la salute del personale

21 ottobre 2009 [doc. *web* n. 1689440]

Pubblicità dei provvedimenti emessi in caso di insussistenza dei presupposti per la proposta di scioglimento dei consigli comunali e provinciali

29 ottobre 2009 [doc. *web* n. 1669219]

Divieto all'uso di dati biometrici per rilevare la presenza sul luogo di lavoro

29 ottobre 2009 [doc. *web* n. 1682066]

Ricorso al Garante e difetto di legittimazione passiva

3 novembre 2009 [doc. *web* n. 1687662]

Prescrizioni concernenti la raccolta d'informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie

12 novembre 2009 [doc. *web* n. 1673588]

Sfruttamento illecito dell'immagine: stop del Garante

12 novembre 2009 [doc. *web* n. 1679779]

No a raccolte indiscriminate sull'Hiv negli studi medici

12 novembre 2009 [doc. *web* n. 1686068]

Gli eredi legittimi possono accedere ai dati bancari del defunto

12 novembre 2009 [doc. *web* n. 1688199]

Linee-guida in tema di referti *online*

19 novembre 2009 [doc. *web* n. 1679033]

Trattamento di dati sensibili e giudiziari presso l'Agenzia autonoma per la gestione dell'albo dei segretari comunali e provinciali

26 novembre 2009 [doc. *web* n. 1679411]

Anagrafe tributaria: proroga dei termini

26 novembre 2009 [doc. *web* n. 1679426]

Dematerializzazione della documentazione clinica

26 novembre 2009 [doc. *web* n. 1688961]

No al *telemarketing* con numeri casuali

3 dicembre 2009 [doc. *web* n. 1679436]

Pubblicazione dell'immagine della figlia minore di una persona nota

10 dicembre 2009 [doc. *web* n. 1691407]

Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale

10 dicembre 2009 [doc. *web* n. 1693019]

Autorizzazione n. 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro

16 dicembre 2009 [doc. *web* n. 1682123]

Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

16 dicembre 2009 [doc. *web* n. 1682956]

Autorizzazione n. 5/2009 al trattamento dei dati sensibili da parte di diverse categorie di titolari

16 dicembre 2009 [doc. *web* n. 1683005]

No alla profilazione occulta

16 dicembre 2009 [doc. *web* n. 1688999]

No a dati sanitari dei dipendenti sui siti delle aziende

16 dicembre 2009 [doc. *web* n. 1689148]

Registri nazionali e regionali degli impianti protesici mammari

16 dicembre 2009 [doc. *web* n. 1689676]

Uso di strumenti informatici e telematici nel processo civile

16 dicembre 2009 [doc. *web* n. 1689683]

Ulteriore differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici rilasciata il 22 febbraio 2007

22 dicembre 2009 [doc. *web* n. 1683067]

Proroga dell'efficacia del provvedimento del 12 marzo 2009, recante prescrizioni ai titolari di banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005

22 dicembre 2009 [doc. *web* n. 1683085]

Illecite alcune foto di George Clooney

22 dicembre 2009 [doc. *web* n. 1686747]

Presentazione di ricorso in via d'urgenza

22 dicembre 2009 [doc. *web* n. 1695163]

Accesso a dati personali relativi a defunti

22 dicembre 2009 [doc. *web* n. 1695325]

Certificati medici: scambio di dati tra Inps e Inpdap

8 gennaio 2010 [doc. *web* n. 1693889]

Modalità di comunicazione dei dati all'interessato

8 gennaio 2010 [doc. *web* n. 1699486]

Oscuramento dell'immagine di una persona non nota

14 gennaio 2010 [doc. *web* n. 1701618]

Assorbimento della tessera sanitaria (Ts) nella carta nazionale dei servizi (Cns)
21 gennaio 2010 [doc. *web* n. 1693904]

Pubblicità degli incarichi conferiti dalle amministrazioni pubbliche
21 gennaio 2010 [doc. *web* n. 1694419]

Sistema di informazione visti (VIS) e scambio di dati fra gli Stati membri dell'Unione europea
28 gennaio 2010 [doc. *web* n. 1694785]

Violenza sessuale e diritto di cronaca
28 gennaio 2010 [doc. *web* n. 1696265]

Propaganda elettorale nel Comune dell'Aquila: impiego degli indirizzi provvisori degli elettori colpiti dal sisma del 2009
4 febbraio 2010 [doc. *web* n. 1694777]

Agenzie matrimoniali e uso dei dati sensibili
4 febbraio 2010 [doc. *web* n. 1700869]

Inammissibilità del ricorso nei confronti della Presidenza del Consiglio-Agenzia informazioni e sicurezza esterna (Aise)
4 febbraio 2010 [doc. *web* n. 1703923]

Misure in materia di propaganda elettorale - esonero dall'informativa
11 febbraio 2010 [doc. *web* n. 1694531]

Violenza sessuale e diritto di cronaca
11 febbraio 2010 [doc. *web* n. 1696239]

Tessera personale di riconoscimento in formato elettronico per il personale della pubblica amministrazione

18 febbraio 2010 [doc. *web* n. 1702885]

Censimento generale dell'agricoltura: trattamento di dati personali e tutela della riservatezza

18 febbraio 2010 [doc. *web* n. 1703119]

Contributi per l'acquisto di *decoder* digitali e trattamento di dati personali

24 febbraio 2010 [doc. *web* n. 1702875]

Utilizzo della posta elettronica e della rete internet presso il Ministero dell'ambiente

4 marzo 2010 [doc. *web* n. 1706464]

Disposizioni in materia di contributo spese per l'esercizio del diritto di accesso ai dati personali conservati nei Sistemi di informazioni creditizie (Sic)

18 marzo 2010 [doc. *web* n. 1708078]

18 marzo 2010 [doc. *web* n. 1709118]

Trattamento dei dati degli abbonati in caso di *number portability*

1° aprile 2010 [doc. *web* n. 1711492]

Provvedimento in materia di videosorveglianza

8 aprile 2010 [doc. *web* n. 1712680]

Misure a tutela della *cd.* "ricerca inversa" dei vecchi abbonati ai servizi telefonici

8 aprile 2010 [doc. *web* n. 1713429]

25. PRINCIPALI ATTIVITÀ INTERNAZIONALI

25.1. UNIONE EUROPEA

COMUNICAZIONI ELETTRONICHE

Direttiva n. 2009/136/CE recante modifica della Direttiva n. 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della Direttiva n. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del Regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

25 novembre 2009 [doc. *web* n. 1707225]

Direttiva n. 2009/140/CE recante modifica delle Direttive n. 2002/21/CE, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, n. 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e n. 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica

25 novembre 2009 [doc. *web* n. 1707229]

PROPOSTA DI ACCORDO UE-USA IN MATERIA DI DATI FINANZIARI (*SWIFT*)

Risoluzione del Parlamento europeo del 17 settembre 2009 sul previsto accordo internazionale sul trasferimento di dati di messaggistica finanziaria al Dipartimento del tesoro degli Stati Uniti d'America per prevenire e combattere il terrorismo e il suo finanziamento

17 settembre 2009 [doc. *web* n. 1714019]

Decisione del Consiglio relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi

20 gennaio 2010 [doc. *web* n. 1718144]

Risoluzione legislativa del Parlamento europeo dell'11 febbraio 2010 sulla proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi

11 febbraio 2010 [doc. *web* n. 1714015]

SPAZIO EUROPEO DI LIBERTÀ, SICUREZZA E GIUSTIZIA

Comunicazione della Commissione *"Uno spazio europeo di libertà, sicurezza e giustizia al servizio dei cittadini"*

10 giugno 2009 [doc. *web* n. 1707817]

Relazione finale del Gruppo di contatto ad alto livello (*High Level Contact Group*) sulla protezione dei dati nei flussi di dati fra Ue ed Usa

23 novembre 2009 [doc. *web* n. 1707249]

Programma di Stoccolma (Consiglio europeo di Stoccolma 2009)

25 novembre 2009 [doc. *web* n. 1707245]

CLAUSOLE CONTRATTUALI *STANDARD*

Decisione della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi a norma della Direttiva n. 95/46/CE

5 febbraio 2010 [doc. *web* n. 1707813]

EURODAC

Proposta modificata della Commissione di modifica del Regolamento relativo al funzionamento dell'EURODAC

10 settembre 2009 [doc. *web* n. 1707254]

Proposta di Decisione del Consiglio relativa all'accesso all'EURODAC da parte delle autorità di contrasto e di EUROPOL

10 settembre 2009 [doc. *web* n. 1707258]

TECNOLOGIA *RFID*

Raccomandazione della Commissione europea sull'attuazione dei princìpi di *privacy* e protezione dati nelle applicazioni supportate dalla tecnologia *Rfid*

12 maggio 2009 [doc. *web* n. 1707262]

25.2. GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del Garante europeo della protezione dei dati sulla relazione finale del Gruppo di contatto ad alto livello Ue-Usa sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale

6 giugno 2009 [doc. *web* n. 1707822]

Parere del Garante europeo della protezione dei dati sulla proposta modificata di Regolamento relativa al funzionamento dell'EURODAC, del 10 settembre 2009, e sulla proposta di Decisione del Consiglio relativa all'accesso ad EURODAC da parte delle autorità di contrasto e di EUROPOL

7 ottobre 2009 [doc. *web* n. 1707268]

Parere del Garante europeo della protezione dei dati sulla Comunicazione della Commissione *"Uno spazio europeo di libertà, sicurezza e giustizia"*

17 novembre 2009 [doc. *web* n. 1707278]

25.3. CORTE DI GIUSTIZIA DELLE COMUNITÀ EUROPEE

TUTELA DELLA RISERVATEZZA DELLE COMUNICAZIONI ELETTRONICHE E NOZIONE DI INTERMEDIARIO

Ordinanza della Corte di giustizia delle Comunità europee nel procedimento C-557/07 (LSG - *Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH* contro *Tele2 Telecommunication GmbH*)

19 febbraio 2009 [doc. *web* n. 1707286]

DIRITTO DI ACCESSO AI DATI E CANCELLAZIONE DEI DATI

Sentenza della Corte di giustizia delle Comunità europee nel procedimento C-553/07 (*College van burgemeester en wethouders van Rotterdam contro M. E. E. Rijkeboer*)

7 maggio 2009 [doc. *web* n. 1707282]

25.4. GRUPPO ART. 29

WP 163 - Parere 5/2009 sui *social network online*

12 giugno 2009 [doc. *web* n. 1707290]

WP 164 - Contributo del Gruppo Art. 29 alla Consultazione pubblica della DG Mercato Interno sulla relazione del Gruppo di esperti in materia di *"credit histories"*

1 dicembre 2009 [doc. *web* n. 1707318]

WP 165 - Parere 6/2009 sul livello della protezione dei dati in Israele

1 dicembre 2009 [doc. *web* n. 1707322]

WP 166 - Parere 7/2009 sul livello della protezione dei dati nel Principato di Andorra

1 dicembre 2009 [doc. *web* n. 1707326]

WP 167 - Parere 8/2009 sulla protezione dei dati dei passeggeri raccolti dai punti di vendita in esenzione da imposte in porti e aeroporti

1 dicembre 2009 [doc. *web* n. 1707331]

WP 168 - Il futuro della *privacy*: contributo congiunto alla Consultazione della Commissione europea sul quadro giuridico relativo al diritto fondamentale alla protezione dei dati personali
1 dicembre 2009 [doc. *web* n. 1707337]

Lettere del Gruppo Art. 29 ai principali operatori di motori di ricerca (*Google, Microsoft, Yahoo!*)
23 ottobre 2009 [doc. *web* n. 1707347]
23 ottobre 2009 [doc. *web* n. 1707351]
23 ottobre 2009 [doc. *web* n. 1707342]

Lettera del Presidente del Gruppo Art. 29 al Direttore della DG Trasporti, Daniel Calleja Crespo, sui *body scanner*. Allegato: Consultazione relativa all'impatto dell'utilizzo di *body scanner* nel settore della sicurezza aerea per quanto riguarda diritti umani, *privacy*, dignità della persona, salute e protezione dei dati
11 febbraio 2009 [doc. *web* n. 1707363]

25.5. SISTEMA INFORMATIVO DOGANALE

Decisione 2009/917/GAI del Consiglio sull'uso dell'informatica nel settore doganale
30 novembre 2009 [doc. *web* n. 1714064]

Parere 03/09 dell'Autorità comune di controllo (Acc) DOGANE sulla proposta di decisione del Consiglio sull'uso dell'informatica nel settore doganale
24 marzo 2009 [doc. *web* n. 1714052]

25.6. 31MA CONFERENZA INTERNAZIONALE DELLE AUTORITÀ DI PROTEZIONE DEI DATI (MADRID, 4-6 NOVEMBRE 2009)

Istruzioni rivolte al Gruppo direttivo istituito dalla Conferenza rispetto alle attività finalizzate ad ottenere lo *status* di osservatore presso lo *Internet Governance Forum*, il *London Action Plan* e l'*ICANN*.

5 novembre 2009 [doc. *web* n. 1707367]

Risoluzione relativa a *standard* internazionali in materia di *privacy*

6 novembre 2009 [doc. *web* n. 1707373]

Risoluzione sul potenziamento della cooperazione internazionale nel settore della *privacy* e della protezione dei dati

6 novembre 2009 [doc. *web* n. 1707377]

Risoluzione relativa all'istituzione di un'Associazione internazionale per la *privacy* (Ipa)

6 novembre 2009 [doc. *web* n. 1707381]

Risoluzione relativa all'istituzione di una settimana internazionale della *privacy* / della protezione dei dati

6 novembre 2009 [doc. *web* n. 1707389]

25.7. GRUPPO DI LAVORO IN MATERIA DI ATTIVITÀ GIUDIZIARIE E DI POLIZIA *WORKING PARTY ON POLICE AND JUSTICE*

Catalogo in materia di cooperazione e controllo nel settore delle attività giudiziarie e di polizia

24 marzo 2009 [doc. *web* n. 1707394]

Comunicato stampa in occasione della pubblicazione delle proposte della Commissione europea relative ad EURODAC

17 settembre 2009 [doc. *web* n. 1707845]

Lettera congiunta WP29-*Wppj* sul progetto di Accordo Ue/Usa relativo al trasferimento dei dati di messaggistica finanziaria (*Swift*)

27 gennaio 2010 [doc. *web* n. 1707398]

25.8. GRUPPO DI LAVORO INTERNAZIONALE SULLA PROTEZIONE DEI DATI NEL SETTORE DELLE TELECOMUNICAZIONI - *IWGDPT*

Raccomandazione sulla protezione dei dati ed i rifiuti elettronici (*e-waste*) - Sofia

12 marzo 2009 [doc. *web* n. 1707402]

Linee-guida sui sistemi di pagamento dei pedaggi stradali - Sofia

12 marzo 2009 [doc. *web* n. 1707406]

Documento di lavoro sul riutilizzo degli *account* di posta elettronica - Berlino

7 settembre 2009 [doc. *web* n. 1714024]