SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Doc. CXXXVI
n. 5

RELAZIONE

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

(ANNO 2011)

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

Presentata dal Garante per la protezione dei dati personali

(SORO)

Comunicata alla Presidenza il 31 ottobre 2012

TIPOGRAFIA DEL SENATO (30)

INDICE

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

II. L'ATTIVITÀ SVOLTA DAL GARANTE

III – L'UFFICIO DEL GARANTE

IV – DOCUMENTAZIONE

ELENCO DELLE ABBREVIAZIONI

La presente Relazione è riferita al 2011 e contiene talune notizie già anticipate nella precedente edizione, nonché alcune ulteriori informazioni, aggiornate all'8 marzo 2012, relative a sviluppi che si è ritenuto opportuno menzionare.

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

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

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

1. Principali interventi dell'Autorità nel 2011 e rapporti istituzionali

1.1. Sintesi di alcuni provvedimenti di particolare rilievo

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

Alcuni pareri resi nel 2011 in relazione ad atti inerenti allo svolgimento di funzioni fondamentali dello Stato sono espressione della complessità applicativa delle norme sulla protezione dati in un contesto normativo e tecnico in rapida evoluzione.

Tecnologie dell'informazione nel processo civile

Con provvedimento 10 giugno 2011 [doc. *web* n. 1822296] nel parere richiesto dal Ministero della giustizia sul provvedimento recante le regole tecniche per l'adozione delle tecnologie dell'informazione nel processo civile e nel processo penale –in attuazione dell'art. 34 del decreto ministeriale 21 febbraio 2011, n. 44– il Garante ha indicato le misure necessarie ad assicurare il rispetto dei princìpi di essenzialità e proporzionalità ed elevare il livello di sicurezza nel trattamento dei dati.

Il favorevole avviso dell'Autorità sul provvedimento è stato subordinato, tra l'altro, alla tassativa indicazione delle infrastrutture facenti parte del sistema informatico del predetto Ministero. È stata poi evidenziata l'opportunità di consentire la condivisione dei soli dati effettivamente pertinenti e necessari all'espletamento di funzioni comuni e, per quanto riguarda "l'area pubblica" del portale dei servizi telematici, di precisare che i dati identificativi dei procedimenti non solo non devono contenere riferimenti in chiaro alle parti, ma neppure permettere di risalire all'identità degli interessati. È stato altresì richiesto un adeguato livello di sicurezza nell'utilizzo dei dispositivi crittografici ai fini dell'identificazione informatica dei soggetti abilitati ad accedere al sistema, nonché di non escludere l'utilizzo di sistemi di

autenticazione forte, non basati cioè solo su *user id* e password. L'Autorità ha ancora sottolineato, per evitare abusi, l'esigenza di prevedere la conservazione dei soli dati realmente necessari ad identificare gli autori degli accessi ai sistemi, entro termini certi, e non indicando solo un termine minimo di conservazione.

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

Le clausole delle convenzioni sono state messe a punto, in piena collaborazione con le parti, per evitare impropri utilizzi dei dati ed assicurare un elevato livello di sicurezza nel trattamento, in entrambi i casi prevedendo che alle banche dati possono accedere solo gli utenti cui sono attribuite specifiche e personali credenziali di abilitazione.

Accesso della Dia alla banca dati dell'Inail relativa ai Durc

Il primo parere (14 aprile 2011 [doc. *web* n. 1813942]) era stato richiesto per l'accesso da parte della Direzione investigativa antimafia (Dia) alla banca dati detenuta dall'Inail relativa ai Documenti unici di regolarità contributiva (Durc), riguardanti gli adempimenti contributivi, previdenziali, assistenziali e assicurativi a carico delle imprese ed indispensabili per la partecipazione a gare d'appalto bandite da soggetti pubblici.

Tale accesso è risultato pertinente all'attività di monitoraggio degli appalti affidata alla Dia dalle vigenti disposizioni (d.lgs. 20 agosto 2002, n. 190, art. 15, confermato dall'art. 180 del d.lgs. 12 aprile 2006, n. 163; decreto del Ministero dell'interno 14 marzo 2003).

Più in particolare, la consultazione della banca dati da parte della Dia è espressamente limitata al monitoraggio degli appalti pubblici; la Dia stessa deve impartire al personale abilitato le istruzioni relative alle responsabilità connesse all'accesso improprio alla banca dati e agli usi illegittimi delle informazioni. La comunicazione tra i sistemi informativi della Dia e dell'Inail avviene attraverso la rete del Sistema pubblico di connettività *SPC/Infranet VPN*, che cifra la comunicazione dalla sorgente alla destinazione e garantisce l'identità delle parti comunicanti. L'Inail provvede al tracciamento degli accessi, che consente di verificare anche le operazioni eseguite da ciascun utente e mette a disposizione della Dia rapporti periodici relativi agli accessi effettuati, nonché a specifici sistemi (*alert*) volti a segnalare in tempo reale anomalie rispetto a parametri predeterminati.

Accesso delle forze di polizia alla banca dati dell'Anagrafe tributaria

La seconda convenzione riguarda l'accesso delle forze di polizia tramite il Centro elaborazione dati (CED), attraverso l'applicativo informatico denominato "Puntofisco", alla banca dati dell'Anagrafe tributaria, in base alla l. 31 maggio 1965, n. 575 che disciplina l'adozione di misure di prevenzione nei confronti degli indiziati di appartenere alla criminalità organizzata e lo svolgimento di indagini sul tenore di vita di tali soggetti e di alcuni familiari. Per tali fini il questore può richiedere ad ogni ufficio pubblico, nonché ad imprese, società ed enti di ogni tipo, informazioni e copia della documentazione ritenuta utile.

Più in dettaglio l'accesso alla banca dati è stato limitato alle sole finalità connesse allo svolgimento delle attività previste dalla normativa sopra indicata, ed ai dati anagrafici, reddituali e fiscali dei soggetti censiti nell'Anagrafe tributaria, escludendo i dati sensibili. Per quanto concerne la sicurezza nel flusso dei dati è stato previsto l'utilizzo del protocollo *"ssl"* per garantire le funzionalità di crittografia dei dati trasferiti da *client* e *server*.

Il parere favorevole dell'Autorità è stato subordinato ad ulteriori integrazioni, volte a sottoporre gli accessi previsti dalla convenzione a monitoraggi, con *alert* per le possibili anomalie, per consentire la verifica delle attività svolte dagli utenti (parere 26 maggio 2011 [doc. *web* n. 1822278]).

1.1.2. Giornalismo e informazione online

Come già lo scorso anno, su segnalazione dell'interessato, pur riconoscendo che rientra nel diritto alla manifestazione del pensiero la pubblicazione di atti giudiziari non più coperti da segreto, è stato vietato ad un sito *web* di continuare a diffondere in rete, nel testo di un'ordinanza di custodia cautelare, dati eccedenti e non essenziali alla finalità informativa perseguita (cfr. art. 137, comma 3, del Codice e art. 6 del codice di deontologia sul trattamento dei dati nell'attività giornalistica - Allegato A.1. al Codice), quali i numeri delle utenze telefoniche oggetto di intercettazioni (provv. 5 maggio 2011 [doc. *web* 1827129]).

1.1.3. Dati genetici e dati relativi allo stato di salute

Autorizzazione generale al trattamento dei dati genetici

Si è riferito nella Relazione 2010 (cfr. pag. 90) che nell'*iter* di aggiornamento dell'autorizzazione generale al trattamento di dati genetici (cfr. art. 90 del Codice), con parere reso al

Ministero della salute, il Consiglio superiore di sanità aveva tra l'altro suggerito di restringere –rispetto all'autorizzazione all'epoca vigente– la categoria delle informazioni genetiche.

Al riguardo l'Ufficio del Garante, svolti i necessari approfondimenti, aveva proposto una differente formulazione. Il Consiglio superiore di sanità nel gennaio 2011 si è espresso in senso favorevole alla definizione di "dato genetico" proposta dal Garante, comprensiva anche delle informazioni relative alle caratteristiche genotipiche di un individuo le quali, pur non essendo il risultato di analisi genetiche, presentano alcune caratteristiche comuni ai dati genetici, tali da rendere opportuna la previsione di particolari cautele nel loro trattamento.

Su tali basi il Garante ha approvato in via definitiva il testo dell'autorizzazione generale (provv. 24 giugno 2011, in G.U. 11 luglio 2011, n. 159 [doc. *web* n. 1822650]), che tiene conto dell'esperienza maturata e delle osservazioni formulate da qualificati esperti, con particolare riferimento, oltre 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'autorizzazione, inoltre, è stata estesa anche agli organismi di mediazione pubblici e privati, introdotti da recente normativa.

Autorizzazione generale al trattamento per scopi di ricerca scientifica

Nel corso dell'anno sono considerevolmente aumentate le richieste di autorizzare trattamenti di dati relativi allo stato di salute, anche in mancanza del consenso degli interessati, a fini di ricerca scientifica, in ragione della giustificata impossibilità di rendere l'informativa ad una parte significativa dei pazienti coinvolti (cfr. art. 110 del Codice).

In tutti i casi è stato autorizzato il trattamento delle sole informazioni indispensabili per lo svolgimento degli studi e sono state individuate diverse precauzioni a tutela della riservatezza dei pazienti coinvolti, quali misure per ridurre il rischio di re-identificazione degli interessati o per impedire ai ricercatori di accedere alla lista di de-codifica detenuta dai medici curanti.

In tale quadro, previa consultazione pubblica per acquisire osservazioni da parte dei soggetti interessati (provv. 15 dicembre 2011), in G.U. 3 gennaio 2012, n. 2 [doc. *web* n. 1859602]), l'Autorità ha adottato un'autorizzazione generale temporanea, che ha tenuto

conto delle più ricorrenti ragioni che hanno reso impossibile fornire l'informativa all'interessato, e, in particolare, dei "motivi etici", ovvero la circostanza nella quale i pazienti che si intende coinvolgere nella ricerca ignorino la propria condizione, ovvero dei "motivi di impossibilità organizzativa", quando risulti impossibile contattare tali soggetti.

L'autorizzazione, adottata in via definitiva il 1° marzo 2012 ([doc. *web* n. 1878276], consente di effettuare studi basati su dati idonei a rivelare lo stato di salute, ovvero ricavati da campioni biologici, raccolti in precedenza a fini di cura o di ricerca, a condizione che sul progetto di ricerca si sia espresso favorevolmente, con parere motivato, il competente comitato etico a livello territoriale.

Per effettuare gli studi in questione sarà necessario adottare misure specifiche (quali tecniche crittografiche, uso di codici identificativi) per non rendere i dati direttamente riconducibili ai pazienti interessati ed informare i pazienti che risultino invece reperibili, acquisendone il consenso al trattamento dei dati. Un elevato livello di sicurezza dovrà essere assicurato in ogni fase della ricerca, adottando opportuni accorgimenti che garantiscano da rischi di accesso abusivo, furto o smarrimento dei supporti di memorizzazione o dei sistemi di elaborazione (ad es. applicando misure di protezione che li rendano inintelligibili a personale non autorizzato). Obbligatorie, infine, le procedure di autenticazione per l'accesso ai dati mediante credenziali di validità limitata alla durata dello studio, la verifica periodica delle credenziali di autenticazione, nonché sistemi di audit log per il controllo degli accessi ed il rilevamento di eventuali anomalie.

Trattamento dati di persone disabili per l'acquisto di un'autovettura

Attiene invece all'utilizzo di dati sensibili nel contesto di attività a carattere economico la deliberazione relativa al trattamento effettuato in occasione dell'acquisto di veicoli per i soggetti disabili, in vista dell'eventuale concessione dei benefici fiscali, adottata su sollecitazione della Federazione italiana dei concessionari di auto (provvedimento 16 febbraio 2011 [doc. *web* n. 1792975]).

Il Garante ha previsto che nelle certificazioni utili per ottenere il beneficio fiscale siano indicati i soli dati pertinenti, e che gli operatori del settore trattino soltanto i dati effettivamente necessari per la definizione della procedura valutativa; in particolare le imprese devono raccogliere la sola documentazione richiesta dalla legge.

L'Autorità ha poi prescritto che i concessionari indichino espressamente agli interessati che i dati forniti potranno essere comunicati ad officine autorizzate per gli eventuali adattamenti da apportare ai veicoli acquistati, provvedendo, in quest'ultimo caso, ad acquisire anche il relativo consenso.

È stato inoltre previsto che, salvo altre esigenze di conservazione (ad es. per controversie giudiziarie pendenti), trascorsi dieci anni, i dati dovranno essere distrutti, cancellati o trasformati in forma anonima. Infine, considerata l'ampiezza e la delicatezza delle informazioni trattate, l'Autorità ha raccomandato ai concessionari, alle imprese e alle officine autorizzate di adottare adeguate misure di sicurezza.

1.1.4. Lavoro

Significativi provvedimenti adottati nel 2011 evidenziano la molteplicità delle vicende attraverso le quali si svolge il rapporto di lavoro e l'esigenza di valutare attentamente la pertinenza dei dati personali utilizzati in tale ambito.

Monitoraggio della navigazione in internet dei dipendenti

Il trattamento dei dati nell'utilizzo dei servizi di comunicazione elettronica nonché l'applicazione dei provvedimenti concernenti il ruolo e le funzioni degli amministratori di sistema nella sicurezza dei trattamenti (provv.ti 27 novembre 2008 [doc. *web* n. 1577499] e 25 giugno 2009 [doc. *web* n. 1626595]), sono stati oggetto di verifica presso una società di primaria rilevanza, con provv. del 21 luglio 2011 [doc. *web* n. 1829641], impugnato davanti al Tribunale di Roma, che ne ha sospeso gli effetti nelle more dello svolgimento del giudizio. All'esito degli accertamenti, l'Autorità ha (tra l'altro) vietato la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione in internet dei dipendenti (tra i quali i tentativi di accesso di ogni singolo dipendente ai domini selezionati, con registrazione dei log indicanti tra l'altro la macchina utilizzata per l'accesso ad internet, indirizzo (*URL*) di destinazione e utente richiedente), ritenendolo in violazione degli artt. 11, comma 1, lett. *a*), *c*) e *d*), 113 e 114 del Codice nonché 4 e 8, l. n. 300/1970. Il *software* utilizzato categorizzava le pagine filtrate classificando i siti visitati e, su base individuale, la navigazione di ciascun utente secondo le categorie predefinite dal sistema medesimo, (quali, ad esempio, quelle denominate *adult material, business and economy, entertainment, abortion,*

militancy and extremist). I dati relativi alla navigazione internet riconducibili ad ogni singolo utente venivano conservati per un minimo di sei mesi, sino ad un anno, in relazione allo spazio disponibile per l'archiviazione.

Alla società è stato prescritto di dare integrale attuazione alla prescrizione di cui alle lett. *c*) ed *f*) del citato provvedimento del 27 novembre 2008, assicurando in particolare che sia resa nota o conoscibile l'identità degli amministratori di sistema nell'ambito della società, nonché la completezza del tracciamento delle attività da essi effettuate.

Utilizzabilità di dati acquisiti in rete in un procedimento disciplinare

In un certo senso speculare è la complessa e delicata vicenda decisa il 6 dicembre 2011, con provvedimento impugnato in sede giurisdizionale [doc. *web* n.1872753], relativa al trattamento di dati sensibili attinenti alla vita sessuale, utilizzati da un ente pubblico per promuovere un procedimento disciplinare a carico di un proprio dipendente. Sulla base della ricostruzione normativa effettuata, con specifico riferimento all'assenza di specifici richiami nel regolamento per il trattamento dei dati sensibili e giudiziari, il Garante ha ritenuto illecito il trattamento effettuato (attraverso l'acquisizione di dati e fotografie su siti internet), vietando pertanto di trattare ulteriormente tali informazioni.

Utilizzo di questionari di personalità

Con provv. 21 luglio 2011 [doc. *web* n. 1825852], impugnato in sede giurisdizionale, il Garante si è espresso in relazione a una procedura di selezione di un dirigente tecnico da parte di un ente pubblico economico, nella quale ai candidati erano stati somministrati, a cura di uno psicologo, *test* di personalità contenenti dettagliate domande relative, fra l'altro, alla sfera affettiva, alla vita sessuale, alle condizioni di salute psico-fisica (con richiesta di indicare la patologia e il medicinale assunto, nonché le visite di natura psicologica/psichiatrica eventualmente effettuate); venivano inoltre richieste informazioni concernenti i disturbi del sonno, abitudini personali relative al fumo, al consumo di alcolici o di droghe ovvero inerenti ad abitudini alimentari o a tentativi di suicidio (effettuati o presi in considerazione dal candidato) nonché a precedenti provvedimenti giudiziari di condanna, e, per le donne, eventuali interruzioni di gravidanza. L'Autorità ha dichiarato illecito il trattamento (per la raccolta di informazioni vietate ai sensi dell'art. 8, l. n. 300/1970 nonché non pertinenti ed eccedenti), con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2, del Codice.

Geolocalizzazione

Data la diffusione degli strumenti volti ad individuare a distanza la posizione geografica degli interessati, è stato adottato un provvedimento generale di bilanciamento di interessi, con il quale sono state impartite alcune prescrizioni ai titolari del trattamento (provv. 4 ottobre 2011 [doc. *web* n. 1850581]). In base al provvedimento i datori di lavoro pubblici e privati possono trattare (senza il consenso dei singoli lavoratori) dati personali ricavati da sistemi di localizzazione per soddisfare esigenze organizzative e produttive, ovvero per la sicurezza sul lavoro nell'ambito della fornitura di servizi di trasporto nonché per commisurare il tempo di lavoro, a condizione che sia data attuazione alla disciplina di protezione dei dati personali ed a quella dettata dall'art. 4, l. n. 300/1970 (Statuto dei lavoratori). Ai lavoratori sottoposti a localizzazione dovranno essere forniti, oltre che gli elementi informativi prescritti dall'art. 13 del Codice, ulteriori ragguagli circa la natura dei dati trattati e le caratteristiche del sistema, da cui risulti con inequivocabile chiarezza che il veicolo è sottoposto a localizzazione. La materia, anche alla luce delle segnalazioni pervenute, ha formato altresì oggetto di attività ispettive, parte delle quali hanno interessato il settore del trasporto pubblico locale, i cui esiti sono, allo stato, in fase di valutazione.

Comunicazione di dati Inail per accertare lo svolgimento del "secondo lavoro"

Un ufficio periferico dell'Inps si è rivolto all'Autorità, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, in relazione ad una richiesta finalizzata alla comunicazione ad un'azienda ospedaliera universitaria di dati concernenti la sussistenza di posizioni previdenziali relative ad un gruppo di lavoratori in un determinato arco temporale. L'azienda intendeva verificare a campione, il rispetto da parte dei propri dipendenti, del divieto di svolgere attività incompatibili con il rapporto di pubblico impiego (cfr. artt. 60-64, d.P.R. n. 3/1957; 53, d.lgs. n. 165/2001 e 1, commi da 56 a 65, l. n. 662/1996).

Il Garante, impregiudicato l'esercizio da parte dell'azienda delle prerogative riconosciute dall'art. 22, l. n. 241/1990, non ha accolto l'istanza presentata, sia per l'assenza di un'espressa previsione normativa che ammettesse detta comunicazione, sia per la presenza di una puntuale disciplina (art. 39, comma 28, l. 27 dicembre 1997, n. 449) che consente di acquisire i dati necessari all'accertamento di eventuali situazioni di incompatibilità mediante la Guardia di finanza (provv. 24 novembre 2011 [doc. *web* n. 1880524]).

1.1.5. Telefonia

Per quanto riguarda la telefonia, l'attività ha riguardato in misura considerevole le chiamate commerciali indesiderate, alla luce dell'istituzione del Registro delle opposizioni nel quale sono iscritte le utenze che non desiderano ricevere telefonate promozionali, a seguito dei provvedimenti dei quali si è già riferito nella Relazione dello scorso anno (p. 9 ss.).

Titolarità del trattamento in capo a chi si avvale di agenti per il *marketing*

In particolare, al fine di chiarire i ruoli dei soggetti che operano nel settore del *telemarketing* l'Autorità ha precisato che deve essere valutato il concreto svolgimento dei rapporti rilevanti in materia di protezione dei dati personali. Occorre quindi considerare come titolare il soggetto in nome o per conto del quale viene effettuata l'attività promozionale, in particolare nel caso in cui lo stesso definisca obiettivi, ad es. elargendo incentivi agli operatori in base ai risultati raggiunti. Il titolare così identificato dovrà anche rispondere di eventuali illeciti. Per queste ragioni, le società che commissionano all'esterno l'attività di promozione ma ne mantengono di fatto il controllo operativo sono tenute anche a designare formalmente responsabili del trattamento i *promoter* o gli agenti di cui si avvalgono (provv. 15 giugno 2011, in G.U. 4 luglio 2011, n. 153 [doc. *web* n. 1821257]; per la proroga dei termini di adempimento delle prescrizioni ivi contenute v. provvedimento del 7 settembre 2011 [doc. *web* n. 1839211]).

Telefonate "mute"

Il Garante si è poi occupato delle cosiddette telefonate "mute", nelle quali il destinatario, dopo aver sollevato il ricevitore, non viene messo in comunicazione con alcun interlocutore, a causa di un sistema automatizzato che consente al singolo operatore l'inoltro di un numero di telefonate superiore alla propria capacità di lavorazione, per eliminare i tempi morti, trasferendo di fatto tempi e costi di attesa sul soggetto chiamato. Con questo sistema la persona chiamata può ricevere una telefonata "muta", reiterata a volte anche nell'arco della medesima giornata, spesso protratta nel tempo e, in difetto di interlocutore, si trova privo di tutele e rimedi.

Al riguardo l'Autorità, al termine di una lunga istruttoria, ha prescritto alla società che si avvaleva di questo sistema una serie di misure e di accorgimenti per impedire la reiterazione di telefonate "mute" ed escludere la possibilità di richiamare lo stesso numero per almeno trenta giorni (provv. 6 dicembre 2011 [doc. *web* n. 1857326]).

Stop a "fax selvaggio"

Appare, infine, di rilievo il provvedimento con il quale è stata ritenuta soggetta all'ambito di applicazione del Codice una società che, sebbene conservasse all'estero i dati personali e li gestisse in modalità remota, utilizzava in modo prevalente un apparato di rete (fax *gateway*) collocato sul territorio italiano. Per tale ragione, l'invio da essa realizzato di fax promozionali senza aver fornito un'idonea informativa né aver acquisito il consenso dell'interessato, è stato dichiarato illecito ed inibito. In ragione del nocumento conseguente all'invio massivo di fax è stata ravvisata la configurabilità, oltre che di illeciti amministrativi, della violazione penale relativa al trattamento illecito di dati (art. 167 del Codice). Il Garante si è inoltre, riservato di verificare la liceità del trattamento operato dalle singole società committenti individuate nel corso degli accertamenti svolti (provv. 7 aprile 2011 [doc. *web* n. 1810207]).

Elenchi telefonici *online*

In relazione a numerose segnalazioni relative alla diffusione sul *web* da parte di una società, di un elenco telefonico *online* contenente anche dati di carattere "riservato", l'Autorità ha ritenuto illecito il trattamento di dati personali posto in essere tramite la costituzione e diffusione del menzionato elenco telefonico se i dati personali contenuti non sono stati tratti dal DBU (*database* telefonico unico, da cui si possono trarre i dati per costituire gli elenchi telefonici, cfr. provv. 15 luglio 2004 [doc. *web* n. 1032381]). Ha altresì affermato che un elenco telefonico basato su una fonte diversa dal DBU non può essere utilizzato per la funzione di "ricerca inversa", cioè per la ricerca del nominativo di un abbonato sulla base del suo numero telefonico, in particolare in mancanza di un consenso espresso dell'interessato a tale funzione (provv. 7 aprile 2011 [doc. *web* n. 1810351]).

1.2. RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI

1.2.1. Le audizioni del Garante in Parlamento

Nel 2011 il Garante ha partecipato ad alcune audizioni presso commissioni parlamentari o altri organismi anche bicamerali su temi all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge, segnalando, nei diversi casi, le implicazioni in ordine al trattamento dei dati personali.

In questo quadro si collocano, in particolare:

a) il 29 novembre 2011, presso la Commissione affari sociali della Camera dei deputati,

un'audizione nell'ambito dell'esame delle proposte di legge recanti disposizioni per consentire l'impianto degli embrioni abbandonati giacenti presso i centri italiani di procreazione medicalmente assistita (A.C. 2058 e abb.). Il Garante si è soffermato in particolare, sulla riconducibilità delle informazioni riguardanti l'embrione alla categoria dei dati personali, sulla disciplina della bio-banca, sulla riservatezza dei donanti gli embrioni, nonché sulla conoscibilità delle condizioni biogenetiche dell'embrione;

b) il 1° giugno 2011, presso la Commissione finanze della Camera dei deputati, un'audizione sulle modifiche al Codice e su altre norme di interesse contenute nel d.l. 13 maggio 2011, n. 70 recante disposizioni urgenti per l'economia. Il Garante ha descritto alcune criticità riscontrate nelle norme di semplificazione contenute nel decreto legge, con particolare riguardo alle limitazioni dell'ambito di applicazione del Codice al trattamento dei dati personali di persone giuridiche, imprese, enti o associazioni; all'esenzione dall'obbligo di acquisizione del consenso dell'interessato nel caso di comunicazioni di dati "infragruppo" nonché all'estensione del regime dell'*opt-in* alla posta cartacea (cfr. par. 2.1.);

c) il 4 maggio 2011, presso la Commissione parlamentare di inchiesta sull'efficacia e l'efficienza del servizio sanitario nazionale, un'audizione relativa all'inchiesta sull'analisi comparativa dell'efficienza, della qualità e dell'appropriatezza delle aziende sanitarie italiane, con riferimento al sistema di codificazione unico a livello nazionale. Il Garante ha analizzato le condizioni affinché l'utilizzo delle banche dati del nuovo sistema informativo sanitario avvenga nel rispetto del diritto alla protezione dei dati personali, richiamando in particolare l'attività consultiva dell'Autorità su taluni provvedimenti istitutivi di particolari sistemi informativi (quali quello sulla salute mentale [doc. *web* n. 1616893] e quello sulle tossicodipendenze [doc. *web* n. 1615306]);

d) il 16 febbraio 2011, presso la Commissione igiene e sanità del Senato, un'audizione nell'ambito dell'indagine conoscitiva sulle malattie ad andamento degenerativo di particolare rilevanza sociale, con specifico riguardo al tumore alla mammella, alle malattie reumatiche croniche ed alla sindrome HIV. Il Garante ha richiamato la disciplina della tutela dei dati personali trattati nell'ambito degli esami diagnostici

relativi alla sindrome HIV, analizzando, in particolare, il d.m. 31 marzo 2008 –che definisce il codice identificativo per la segnalazione– e il d.lgs. n. 16/2010, che ha disposto l'obbligatorietà dell'analisi clinica in caso di trapianto di tessuti e cellule umane, al fine di impedire la trasmissione del virus HIV.

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

Nel 2011 l'Autorità ha fornito la consueta collaborazione al Governo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

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

a) interrogazione n. 4-12195 concernente la somministrazione, ai partecipanti alla procedura indetta da un ente pubblico economico per selezionare un dirigente tecnico, di un *test* relativo ad aspetti anche intimi della sfera personale. Il caso oggetto dell'interrogazione era stato esaminato sulla base di notizie di stampa dal Garante che, con provvedimento oggetto di impugnazione in sede giurisdizionale, ha vietato il trattamento dei dati personali comunque ricavati dalla somministrazione dei *test* (provv. 21 luglio 2011 [doc. *web* n. 1825852]), riservandosi di valutare con autonomo procedimento la sussistenza di eventuali violazioni amministrative. Copia del provvedimento è stata trasmessa all'autorità giudiziaria per le valutazioni in ordine agli illeciti penali eventualmente ravvisabili e al Ministero del lavoro e delle politiche sociali per le valutazioni di competenza (nota 16 novembre 2011; per ulteriori dettagli sul caso v. par. 10.3.);

b) interpellanza n. 2-00170 concernente l'acquisizione indebita di intercettazioni o immagini. Nella nota del 28 luglio 2011, inviata alla Presidenza del Consiglio dei ministri, sono stati citati i diversi provvedimenti con i quali il Garante si è espresso in argomento e, in particolare, in materia di pubblicazione del contenuto di intercettazioni giudiziarie. Così nel provvedimento del 21 giugno 2006 (in G.U. 27 giugno 2006, n. 147 [doc. *web* n. 1299615]), il Garante, richiamando gli operatori della stampa

al rispetto delle norme vigenti, ha sottolineato che occorre garantire il diritto all'informazione su fatti di interesse pubblico nel rispetto dell'essenzialità dell'informazione stessa (v. relazione 2006, pp. 4, 76 ss.).

Con riferimento invece alla pubblicazione di foto e immagini realizzate in casa o altri luoghi di privata dimora, si è ricordato che il Garante, anche a seguito di segnalazioni, accertata l'illiceità del trattamento, ha vietato l'ulteriore diffusione delle immagini acquisite qualora: le modalità di ripresa delle immagini fotografiche e la loro successiva pubblicazione concretizzino "condotte illecite legate alla tutela del domicilio"; le immagini contengano dati personali relativi a persone riprese con un uso non corretto di una tecnica invasiva (teleobiettivo); il trattamento di tali immagini, a partire dall'iniziale raccolta sino alla loro pubblicazione, risulti illecito alla luce delle disposizioni in materia di protezione dei dati personali e del codice di deontologia;

c) interrogazione n. 4-08954 concernente la tutela nei confronti della immotivata disabilitazione dei profili degli utenti all'interno del *social network Facebook*. L'Autorità ha rilevato che le sue possibilità di intervento in materia sono in certa misura circoscritte in ragione dei limiti territoriali che l'applicazione della normativa italiana incontra rispetto a trattamenti effettuati in luoghi non soggetti alla sovranità dello Stato italiano. Ha poi richiamato i diversi casi nei quali, essendo stato lamentato il trattamento illecito di dati personali su *Facebook,* ha contattato il titolare del trattamento in una prospettiva di collaborazione (nota 22 dicembre 2011), (cfr. per i dettagli Relazione 2010, pp. 111-113);

d) interrogazione n. 3-01984, concernente il Registro pubblico delle opposizioni (v. al riguardo par. 9.1.). Il Garante, nel ricostruire l'evoluzione della specifica normativa (su cui v. Relazione 2010, p. 9 ss.), ha avuto modo di rilevare alcune criticità nel funzionamento del Registro, evidenziate dalla rilevanza delle segnalazioni pervenute e ha richiamato il provvedimento generale sulla "Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali", con cui è stata sottolineata l'esigenza di una maggiore chiarezza in ordine ai rapporti tra titolare e responsabile del trattamento, con particolare riguardo alle ipotesi di

affidamento delle attività promozionali in *outsourcing* (provv. 15 giugno 2011 [doc. *web* n. 1821257], nota 21 dicembre 2011).

1.2.3. L'attività consultiva del Garante sugli atti del Governo

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso anche nel 2011 (oltre a quelli menzionati nella Relazione 2010, pp. 15-16), e nel primo scorcio del 2012, diversi pareri, i quali hanno riguardato, in particolare:

1. uno schema di ordinanza di necessità e urgenza del Ministro della salute relativa all'adozione di ulteriori provvedimenti in materia di protesi mammarie (PIP) (parere 1° marzo 2012 [doc. *web* n. 1881229]);
2. uno schema di decreto del Presidente del Consiglio dei ministri concernente iscrizione agli elenchi dei fornitori qualificati del Sistema pubblico di connettività (SPC), ai sensi del codice dell'amministrazione digitale (CAD) (parere 12 gennaio 2012 [doc. *web* n. 1872045]);
3. uno schema di ordinanza di necessità e urgenza del Ministro della salute, relativa all'adozione di provvedimenti in materia di protesi mammarie cosiddette PIP (parere 29 dicembre 2011 [doc. *web* n. 1863619]);
4. uno schema di regolamento del Ministro della giustizia che apporta modifiche ed integrazioni al decreto del Ministro della giustizia 21 febbraio 2011, n. 44 recante "Regolamento concernente le 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 d.lgs. 7 marzo 2005, n. 82 e successive modificazioni, ai sensi dell'art. 4, commi 1 e 2, del d.l. 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla l. 22 febbraio 2010, n. 24" (parere 21 dicembre 2011 [doc. *web* n. 1870802]);
5. uno schema di regolamento del Ministro dell'economia e delle finanze che integra il d.m. 29 novembre 2007, n. 255, recante regolamento di attuazione degli artt. 20, 21 e 181 del Codice (parere 15 dicembre 2011 [doc. *web* n. 1882020]);

6. uno schema di decreto del Presidente del Consiglio dei ministri in materia di separati certificati di firma (parere 24 novembre 2011 [doc. *web* n. 1870611]);
7. uno schema di decreto del Presidente del Consiglio dei ministri recante regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli artt. 20, comma 3; 24, comma 4; 28, comma 3; 32, comma 3, lett. *b*); 35, comma 2; 36, comma 2 e 71, del codice dell'amministrazione digitale (parere 24 novembre 2011 [doc. *web* n. 1870620]);
8. uno schema di decreto del Presidente del Consiglio dei ministri recante regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata (parere 24 novembre 2011 [doc. *web* n. 1870629]);
9. uno schema di regolamento del Ministro dell'economia e delle finanze, concernente il tirocinio dei revisori legali, in applicazione dell'art. 3 del d.lgs. n. 39/2010 recante attuazione della Direttiva n. 2006/43/CE (parere 10 novembre 2011 [doc. *web* n. 1851797]);
10. uno schema di regolamento del Ministro dell'economia e delle finanze, concernente il contenuto e le modalità di iscrizione nonché i casi e le modalità di cancellazione dal registro dei revisori legali e delle società di revisione, in applicazione dell'art. 6 del d.lgs. n. 39/2010 recante attuazione della Direttiva n. 2006/43/CE (parere 10 novembre 2011 [doc. *web* n. 1851772]);
11. uno schema di regolamento del Ministro dell'economia e delle finanze, concernente i requisiti per l'iscrizione al registro dei revisori legali in applicazione dell'art. 2, commi 2, 3, 4 e 7, e dell'art. 7, comma 7, del d.lgs. n. 39/2010 recante attuazione della Direttiva n. 2006/43/CE (parere 10 novembre 2011 [doc. *web* n. 1851757]);
12. uno schema di linee di indirizzo del Ministero dell'economia e delle finanze sui ticket regionali per fasce di reddito (parere 26 ottobre 2011 [doc. *web* n. 1851679]);
13. uno schema di linee-guida di Digit-Pa in materia di "*Disaster Recovery* delle pubbliche amministrazioni" (parere 20 ottobre 2011 [doc. *web* n. 1851672]);
14. uno schema di decreto del Ministro della salute recante "Istituzione del sistema informativo per il monitoraggio dell'assistenza erogata presso gli *hospice*" (parere 11 ottobre 2011 [doc. *web* n. 1851388]);

15. uno schema di decreto del Presidente della Repubblica recante modifiche al regolamento in materia di ordinamento militare (d.P.R. n. 90/2010) (parere 22 settembre 2011 [doc. *web* n. 1844183]);
16. uno schema di convenzione tra Ministero dell'interno - Centro coordinamento nazionale per la viabilità e gli operatori dei servizi di comunicazione elettronica, per la fornitura del servizio di invio di messaggi nelle situazioni di crisi della viabilità nazionale (parere 15 settembre 2011 [doc. *web* n. 1844167]);
17. uno schema di decreto del Ministro del lavoro e delle politiche sociali recante norme in materia di sperimentazione, in favore degli enti caritativi, del programma "carta acquisti" (parere 27 luglio 2011 [doc. *web* n. 1832767]);
18. una bozza di ordinanza del Presidente del Consiglio dei ministri recante "Ulteriori disposizioni urgenti dirette a fronteggiare lo stato di emergenza umanitaria nel territorio nazionale in relazione all'eccezionale afflusso di cittadini appartenenti ai Paesi del Nord Africa" (parere 14 luglio 2011 [doc. *web* n. 1826722]);
19. uno schema di decreto interministeriale recante le "Regole tecniche per la realizzazione e il funzionamento del Sistema informativo per la prevenzione nei luoghi di lavoro (SINP), nonché le regole per il trattamento dei dati, ai sensi dell'art. 8, comma 4, del d.lgs. 9 aprile 2008, n. 81" (parere 7 luglio 2011 [doc. *web* n. 1829704]);
20. una versione preliminare delle linee-guida della Presidenza del Consiglio dei ministri - Dipartimento funzione pubblica sui siti *web* delle pubbliche amministrazioni del Ministro per la pubblica amministrazione e l'innovazione (parere 7 luglio 2011 [doc. *web* n. 1826713]);
21. uno schema di decreto del Ministro dell'istruzione dell'università e della ricerca sulle modalità e i contenuti della prova di ammissione ai corsi di laurea magistrale in medicina e chirurgia in inglese (parere 7 luglio 2011 [doc. *web* n. 1826705]);
22. uno schema di decreto del Ministro dell'interno recante il nuovo regolamento di gestione dell'Indice nazionale delle anagrafi (INA) (parere 24 giugno 2011 [doc. *web* n. 1826698]);

23. uno schema-tipo di documento progettuale del Ministro per la pubblica amministrazione e l'innovazione per la produzione, il rilascio e la gestione del modello ATE da parte delle amministrazioni dello Stato in attuazione dell'art. 4, del d.P.C.m. del 24 maggio 2010, recante regole tecniche delle tessere di riconoscimento (mod. ATE) di cui al d.P.R. n. 851/1967, rilasciate con modalità elettronica dalle amministrazioni dello Stato, ai sensi dell'art. 66, comma 88 del d.lgs. n. 82/2005 (parere 10 giugno 2011 [doc. *web* n. 1822311]);
24. uno schema di provvedimento del Ministero della giustizia recante specifiche tecniche di cui all'art. 34 del decreto del Ministro della giustizia del 21 febbraio 2011, n. 44, recante regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione ai sensi dell'art. 4, comma 1, d.l. n. 193/2009, convertito dalla l. n. 24/2010 (parere 10 giugno 2011 [doc. *web* n. 1822296]);
25. uno schema di decreto del Ministro dello sviluppo economico recante regolamento relativo alla designazione e nomina dei componenti del consiglio ed all'elezione dei membri della giunta delle Camere di commercio, in attuazione dell'art. 12, della l. 29 dicembre 1993, n. 580, così come modificata dal d.lgs. 15 febbraio 2010, n. 23; (parere 26 maggio 2011 [doc. *web* n. 1817531]);
26. 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 (parere 26 maggio 2011 [doc. *web* n. 1890457]);
27. uno schema di decreto del Presidente della Repubblica recante "Regolamento di attuazione in materia di risoluzione del rapporto di lavoro dei dipendenti delle amministrazioni pubbliche dello Stato e degli enti pubblici nazionali in caso di permanente inidoneità psicofisica ai sensi dell'art. 55-*octies* del d.lgs. 30 marzo 2001, n. 165" (parere 19 maggio 2011 [doc. *web* n. 1890453]);
28. uno schema di decreto del Presidente della Repubblica recante modifica delle disposizioni in materia di stato civile relativamente alla disciplina sul cognome contenuta nel d.P.R. 3 novembre 2000, n. 396 (parere 27 aprile 2011 [doc. *web* n. 1816423]);

29. uno schema di provvedimento di Digit-Pa recante regole tecniche ai sensi dell'art. 6, comma 1-*bis* del codice dell'amministrazione digitale per l'estrazione di caselle PEC ai sensi degli artt. 16, comma 10 e 16-*bis*, comma 5, del d.l. 29 novembre 2008, n. 185, convertito, con modificazioni, dalla l. 28 gennaio 2009, n. 2 (parere 21 aprile 2011 [doc. *web* n. 1807547]);
30. uno schema di decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le preiscrizioni universitarie per l'anno accademico 2011/2012 (parere 7 aprile 2011 [doc. *web* n. 1807556]);
31. uno schema di decreto del Ministro della difesa concernente le modalità di caricamento dei dati sanitari di emergenza nella tessera personale di riconoscimento del personale militare, i livelli e le modalità di accesso selettivo ai dati, nonché le specifiche misure volte a garantire la sicurezza, adottato ai sensi dell'art. 1496, comma 2, del d.lgs. 15 marzo 2010, n. 66 (Carta Multiservizi Difesa - CMD) (parere 16 febbraio 2011 [doc. *web* n. 1797055]);
32. uno schema di decreto del Ministro del lavoro e delle politiche sociali di modifica del decreto interministeriale 4 febbraio 2010 concernente i criteri e le modalità per la ripartizione fra le regioni e le province autonome delle disponibilità del fondo per il diritto al lavoro dei disabili di cui all'art. 13, della l. 12 marzo 1999, n. 68 (parere 3 febbraio 2011 [doc. *web* n. 1790408]).

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

1) il decreto del Presidente della Repubblica 15 dicembre 2011, n. 233 (in G.U. 29 febbraio 2012, n. 50), recante regolamento in materia di disciplina sui flussi informativi necessari per l'esercizio dei compiti attribuiti all'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata, nonché delle modalità delle comunicazioni, da effettuarsi per via telematica, tra la predetta Agenzia e l'autorità giudiziaria, a norma dell'art. 113, comma 1, lett. *c*), del d.lgs. 6 settembre 2011, n. 159;

2) il decreto 10 gennaio 2012 del Ministero delle infrastrutture e dei trasporti (in G.U. 14 gennaio 2012, n. 11), recante disposizioni di attuazione dell'art. 11, commi 1 e 2, punto 1, del decreto 25 novembre 2011 in materia di registro elettronico nazionale delle imprese che esercitano la professione di trasportatore su strada;
3) il decreto 15 novembre 2011 del Ministro della salute (in G.U. 14 gennaio 2012, n. 11), recante definizione dei requisiti minimi per le organizzazioni di ricerca a contratto (CRO) nell'ambito delle sperimentazioni cliniche di medicinali;
4) il decreto 13 ottobre 2011 del Ministro del lavoro e delle politiche sociali (in G.U. 2 gennaio 2012, n. 1), che definisce *standard* e regole per la trasmissione informatica di dati alla borsa continua nazionale del lavoro denominata "Cliclavoro";
5) il decreto 20 settembre 2011 del Ministro del lavoro e delle politiche sociali (in G.U. 3 dicembre 2011, n. 282), recante modalità di interconnessione a "Cliclavoro" di università e altri soggetti autorizzati all'esercizio dell'attività di intermediazione;
6) il decreto 2 novembre 2011 del Ministero dell'economia e delle finanze (in G.U. 12 novembre 2011, n. 264), recante la dematerializzazione della ricetta medica cartacea, di cui all'art. 11, comma 16, del d.l. n. 78/2010 (Progetto Tessera Sanitaria);
7) il decreto del Presidente della Repubblica 14 settembre 2011, n. 179 (in G.U. 11 novembre 2011, n. 263), recante regolamento concernente la disciplina dell'accordo di integrazione tra lo straniero e lo Stato, a norma dell'art. 4-*bis*, comma 2, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al d.lgs. 25 luglio 1998, n. 286;
8) l'ordinanza 1° ottobre 2011, n. 3697 del Presidente del Consiglio dei ministri (in G.U. 11 ottobre 2011, n. 237), recante disposizioni urgenti di protezione civile, limitatamente all'art. 10, il quale prevede la trasmissione, da parte delle società di gestione dei sistemi di telefonia mobile, ai titolari di utenze presenti a New York durante il passaggio dell'uragano "Irene", di informazioni dirette a fornire assistenza ai cittadini presenti;
9) il decreto direttoriale 9 settembre 2011 del Ministero dell'economia e delle finanze (in G.U. 6 ottobre 2011, n. 233), recante nuove disposizioni per l'istituzione dell'elenco

pubblico in materia di apparecchi e terminali da intrattenimento di cui all'art. 1, comma 82, della l. n. 220/2010 (si segnala, in particolare, che l'art. 7 prevede, ai fini dell'iscrizione all'elenco, la comunicazione del consenso al trattamento dei dati personali ai sensi del Codice);

10) il decreto 21 aprile 2011 del Ministro della salute (in G.U. 17 settembre 2011, n. 217), recante nuove modalità per gli adempimenti previsti dall'art. 5, commi 5, 5-*quinquies* 1 e 5-*quinquies* 2 del d.lgs. n. 507/1992 e dall'art. 15, commi 5-*bis* e 5-*ter* del d.lgs. n. 46/1997, relativamente alle comunicazioni che gli organismi notificati aventi sede legale in Italia, autorizzati a certificare determinati dispositivi medici, sono tenuti a trasmettere al Ministero della salute;

11) l'intesa 27 luglio 2011, n. 134/CSR (in G.U. 18 agosto 2011, n. 191), ai sensi dell'art. 8, comma 6, della l. 5 giugno 2003, n. 131, tra il Governo, le Regioni e le Province autonome di Trento e Bolzano concernente il "Documento di consenso sulle politiche di offerta e le modalità di esecuzione del *test* per HIV in Italia";

12) il provvedimento del 30 giugno 2011 del Ministero dell'economia e delle finanze (in G.U. 13 luglio 2011, n. 161), recante la determinazione delle informazioni, dei dati e delle contabilità relativi alle attività di gioco che i soggetti titolari di concessione dell'esercizio e raccolta non a distanza dei giochi pubblici trasmettono al sistema centrale dell'Amministrazione autonoma dei monopoli di Stato;

13) l'accordo 5 maggio 2011, n. 44/CU, (in G.U. 1° giugno 2011, n. 121), ai sensi dell'art. 9 del d.lgs. 28 agosto 1997, n. 281, tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano e gli enti locali sul documento "Linee di indirizzo per l'assistenza alle persone in stato vegetativo e stato di minima coscienza", (Rep. n. 44/CU);

14) l'ordinanza contingibile ed urgente 14 aprile 2011 (in G.U. 18 maggio 2011, n. 114), relativa alla tutela delle persone maggiormente sensibili agli effetti delle ondate di calore;

15) l'accordo 20 aprile 2011, n. 75/CSR (in G.U. 17 maggio 2011, n. 113), ai sensi dell'art. 6, comma 1, del d.lgs. 6 novembre 2007, n. 191, tra il Governo, le Regioni e

le Province autonome di Trento e Bolzano sul documento recante: "Linee-guida per l'accreditamento delle banche di sangue da cordone ombelicale";

16) il decreto 31 gennaio 2011 del Ministero delle infrastrutture e dei trasporti (in G.U. 16 febbraio 2011, n. 38), recante modalità di trasmissione della certificazione medica per il conseguimento e il rinnovo della patente di guida.

1.2.4. Altri pareri

a) L'Autorità ha reso parere sullo schema di decreto legislativo recante "Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione" (parere 15 giugno 2011 [doc. *web* n. 1826687]) che, nella parte di specifico interesse, teneva conto di alcune indicazioni rese dall'Ufficio del Garante a rappresentanti del Ministero della giustizia nel corso di contatti informali a fini di collaborazione.

Le norme, nel ricondurre –in ossequio al criterio di delega di cui all'art. 54, comma 4, lett. *b*), n. 1, della l. 18 giugno 2009, n. 69– i procedimenti in cui sono prevalenti caratteri di *"concentrazione processuale, ovvero di officiosità dell'istruzione"* al rito del lavoro, annoverano fra questi anche il procedimento relativo all'applicazione delle disposizioni del Codice in materia di protezione dei dati personali (art. 152).

Le disposizioni di specifico interesse per la protezione dei dati (art. 10) e le modifiche apportate al Codice, nonché in particolare al predetto art. 152, sono descritte al paragrafo 2.1.6.

In questa sede, si segnala soltanto che il giudice territorialmente competente –secondo quanto già previsto dal Codice– si individua in ragione del luogo in cui ha la residenza il titolare del trattamento (art. 10, comma 2, del citato schema).

Nel parere, sulla base dell'esperienza applicativa maturata in questi anni, il Garante ha suggerito, quale ulteriore criterio regolativo della competenza, anche il luogo di residenza del responsabile o dell'incaricato del trattamento, ove risultino destinatari del provvedimento. L'osservazione del Garante non è stata, però, recepita nel testo del decreto legislativo, approvato definitivamente dal Consiglio dei ministri.

1.3. LEGGI REGIONALI

Nel 2011 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 (32) è stato riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale rispetto ai profili di protezione dei dati personali.

Solo in un caso l'Autorità ha formulato osservazioni sulla compatibilità della legge con le disposizioni in materia di protezione dei dati personali –assunte quali norme interposte ai fini del sindacato di costituzionalità (v. Corte Cost. n. 271/2005)– per fornire elementi utili a valutare l'eventuale sussistenza dei presupposti necessari all'impugnazione della legge regionale. Si tratta, in particolare, della legge della Regione Calabria n. 37 del 7 ottobre 2011, recante "Modifica alle leggi regionali 13 maggio 1996, n. 7 e 13 maggio 1996, n. 8 - Pubblicità della situazione patrimoniale dei dirigenti della Regione Calabria". Gli elementi di criticità riscontrati attengono, in particolare, alla dubbia compatibilità degli obblighi di pubblicità della situazione patrimoniale e tributaria dei dirigenti della giunta regionale, con i princìpi di necessità e di pertinenza di cui agli artt. 3, 11 e 22, comma 8, del Codice. La legge –che estende gli obblighi di pubblicità previsti dalla legge regionale n. 24/2010, in relazione alla quale il Garante aveva già manifestato la propria perplessità– prevede, in particolare, la pubblicazione integrale delle dichiarazioni dei redditi degli interessati, così finendo per legittimare la diffusione di dati non strettamente pertinenti rispetto alle finalità della legge. Sono state inoltre ravvisate talune criticità nell'estensione degli obblighi di pubblicità della situazione patrimoniale alla dirigenza che, in quanto tale, sembra esclusa dall'alveo soggettivo di applicazione delle leggi emanate dalle regioni in attuazione di quanto sancito dall'art. 15 della l. n. 441/1982. Il motivo di tale esclusione sembrerebbe del resto riconducibile alla *ratio* stessa dell'istituto dell'anagrafe patrimoniale, concepito quale espressione del rapporto di rappresentanza e del controllo democratico, da parte dei cittadini, in ordine alle attività e alle condizioni soggettive degli eletti rilevanti ai fini dell'esercizio del mandato. Tale *ratio* non sembra invece estensibile a pubblici dipendenti –quali i dirigenti– la cui attività si presenta di per sé come estranea ad ogni rapporto, diretto o indiretto, di rappresentanza (nota 16 novembre 2011).

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 della persona rispetto al trattamento dei dati che la riguardano e in particolare del *"diritto alla protezione dei dati personali"*.

Pur nel sostanziale rispetto del suo impianto generale, il Codice ha subito nel corso del 2011 talune significative modifiche, che di seguito si espongono.

2.1.1. Gli enti quali soggetti di diritto ai fini della disciplina in materia di protezione dei dati personali

Tra le innovazioni maggiormente significative vanno considerate, in primo luogo, quelle di cui all'art. 40, comma 2, del d.l. 6 dicembre 2011, n. 201 (cd. "salva-Italia"), convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, che ha ridisegnato la disciplina in materia di protezione dei dati personali nella parte inerente il trattamento di dati relativo a persone giuridiche, enti o associazioni.

La norma ha inciso sulla materia a breve distanza da una precedente novella, che aveva già esentato in parte tali trattamenti dall'applicazione delle regole e delle garanzie poste a protezione dei dati personali, nel tentativo di semplificare gli adempimenti gravanti sulle imprese (d.l. 13 maggio 2011 n. 70, convertito, con modificazioni, dalla l. 12 luglio 2011, n. 106; cd. "decreto sviluppo"). Tale ultimo provvedimento, in particolare, aveva aggiunto all'art. 5 del Codice un comma 3-*bis*, secondo cui: *"Il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo contabili, come definite all'art. 34, comma 1-ter, non è soggetto all'applicazione del presente codice"*.

L'esclusione dall'ambito di applicazione del Codice del *"trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni"* era volta, come può leggersi nella relazione illustrativa del decreto legge, a *"ridurre gli oneri derivanti dal trattamento di dati*

nell'ambito di rapporti di natura meramente amministrativa o economica tra imprese e tra queste ed enti pubblici, senza alterare in alcun modo i livelli di tutela garantiti dal codice alle persone fisiche".

L'esclusione, stando alla formulazione della norma non operava:

a) se il trattamento effettuato da *"persone giuridiche, imprese, enti o associazioni"* avesse riguardato dati di persone fisiche;

b) se fosse avvenuta al di fuori dei rapporti intercorrenti fra *"persone giuridiche, imprese, enti o associazioni"* (ad esempio, fra una persona giuridica e una persona fisica);

c) se fosse avvenuta per finalità diverse da quelle *"amministrativo contabili"* (cfr. *infra*).

A seguito della novella apportata dal d.l. 6 dicembre 2011, n. 201 le nozioni stesse di "dato personale" e di "interessato" (art. 4, comma 1, lettere *b*) e *i*) del Codice) non si riferiscono più alle "persone giuridiche", né agli "enti o associazioni".

La portata dell'intervento normativo è molto significativa e suscita almeno tre considerazioni:

a) la finalità delle disposizioni è individuata (come già, nel d.l. n. 70/2011) nella *"riduzione degli oneri in materia di privacy"*, in termini che presentano le misure in materia di protezione dei dati personali esclusivamente quali "oneri" o "adempimenti amministrativi per le imprese" da ridurre, se non da eliminare completamente, attraverso reiterati interventi legislativi, piuttosto che come un *corpus* normativo posto a tutela dei diritti dei cittadini;

b) le nuove misure esentano le imprese da ogni adempimento previsto dalla normativa in materia di protezione dei dati personali (richiesta del consenso dell'interessato, ove necessario, informativa, adozione delle misure di sicurezza, ecc.), ma solo quando il trattamento di dati non riguarda persone fisiche (e non potrebbe essere altrimenti, a pena di contrasto con la normativa dell'Unione europea), sicché hanno, in sostanza, una portata necessariamente limitata;

c) l'intervento normativo si sostanzia nell'"azzeramento" della tutela delle persone giuridiche rispetto al trattamento dei dati che le riguardano, comportando l'impossibilità per le stesse di usufruire degli strumenti che il Codice prevede e in particolare, del

diritto di accesso e degli altri diritti di cui all'art. 7 (rettifica, cancellazione, ecc.) che, fino ad oggi, hanno consentito a un copioso numero di soggetti giuridici di conoscere i dati personali che li riguardano e di intervenire sugli stessi, in diversi ambiti, laddove erronei, non aggiornati, eccedenti o trattati in violazione di legge. A conferma di ciò, si rileva che numerosi sono stati i ricorsi, i reclami e le segnalazioni pervenuti nel tempo all'Autorità proprio da parte di persone giuridiche, soprattutto piccole e medie imprese, che, in presenza di trattamenti illeciti dei propri dati, lamentavano conseguenze negative anche sulla propria attività economica (quali, ad esempio, impossibilità di accedere al mercato del credito, di partecipare a gare di appalto, di poter usufruire di beni e servizi necessari allo svolgimento della propria attività, ecc.). Si consideri infine che –sulla scia di quanto già disposto dal cd. "decreto sviluppo"– la novella al Codice priva di tutela anche quelle particolari organizzazioni che sono i partiti e le ONLUS.

A fronte della suddetta novella delle lettere *b*) e *i*) del comma 1 dell'art. 4, il d.l. "salva-Italia" non è, per altro verso, intervenuto su altre disposizioni del Codice (Titolo X - Comunicazioni elettroniche) dedicate al trattamento di dati connesso alla fornitura di servizi di comunicazione elettronica. In particolare, non è stato modificato l'oggetto della definizione di "abbonato" a tali servizi di comunicazione elettronica, pure contenuta nel Codice, che risulta perciò tuttora applicabile tanto alle persone fisiche quanto a quelle giuridiche (art. 4, comma 2, lett. *f*) del Codice).

La mancata esclusione delle persone giuridiche dalla nozione di "abbonato" si conforma del resto al quadro normativo europeo e, in particolare, alla Direttiva n. 2002/58/CE (recentemente modificata dalla Direttiva n. 2009/136/CE) in base alla quale *"gli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico possono essere persone fisiche o persone giuridiche"* (considerando 12) e che prevede *"la tutela dei legittimi interessi degli abbonati che sono persone giuridiche"* (art. 1, par. 2).

Pertanto, le persone giuridiche, gli enti e le associazioni, in quanto abbonati a un servizio di comunicazione elettronica, dovrebbero poter continuare a fruire ancora delle garanzie previste dal Titolo X del Codice.

Tale soluzione –la sola, del resto, conforme all'obbligo di interpretazione adeguatrice del diritto interno al diritto dell'Unione europea– non emerge tuttavia con chiarezza dal testo delle disposizioni del Codice, posto che il Titolo X riguarda comunque il trattamento di "dati personali", con esclusione, dunque, dei dati relativi alle persone giuridiche, giusta la novella apportata dal d.l. n. 201/2011 (art. 121 del Codice). Non solo, ma anche le tutele amministrative innanzi al Garante continuano ad essere riconosciute solo agli "interessati", con esclusione ancora una volta, a seguito della nuova definizione, delle persone giuridiche e degli altri soggetti assimilati (art. 141 del Codice).

Per tali ragioni, l'Autorità ha segnalato al Governo (mediante una nota, inviata al Ministro dello sviluppo economico, quale titolare del dicastero "capofila" nell'attuazione della predetta Direttiva n. 2009/136/CE, rilevante in materia) l'opportunità di delineare con chiarezza ed alla luce della normativa europea il quadro normativo riferibile alla figura dell'abbonato-persona giuridica, in particolare per quanto riguarda le garanzie e le forme di tutela che si intendono riservare a questi soggetti (diritto di accesso a propri dati personali, diritto di opposizione, ecc.) (nota 24 febbraio 2012).

2.1.2. Casi di esenzione dall'obbligo di acquisizione del consenso

Il d.l. 13 maggio 2011, n. 70 ha apportato altre significative modifiche (tuttora vigenti) al Codice, in relazione alle ipotesi di esenzione dall'obbligo di acquisizione del consenso al trattamento dei dati personali da parte di soggetti privati o enti pubblici economici. Si segnalano, di seguito, le più rilevanti:

1) il trattamento dei dati contenuti in *curricula* spontaneamente trasmessi

   L'art. 6, comma 2, lett. *a*), nn. 2, 3 e 4 del decreto legge reca una disciplina derogatoria per il trattamento dei dati contenuti in *curricula* spontaneamente trasmessi dall'interessato (ovvero sollecitati dal ricevente), al fine di eliminare "*adempimenti privi di utilità sul piano pratico e ingiustificati ai fini della tutela dei dati, in quanto imposti dalla legge nonostante che il candidato acconsenta spontaneamente al trattamento dei propri dati personali per finalità occupazionali*" (così si legge nella relazione illustrativa del d.d.l. di conversione del decreto legge).

In particolare, in primo luogo, con puntuali novelle agli artt. 24 e 26 del Codice, si prevedono:

a) l'esonero dall'obbligo di richiedere il consenso per il trattamento dei dati comuni contenuti nei *curricula* spontaneamente trasmessi, per l'eventuale instaurazione di un rapporto lavorativo;

b) l'esonero dall'obbligo di richiedere il consenso scritto dell'interessato e di ottenere l'autorizzazione del Garante, per il trattamento dei dati sensibili contenuti nei *curricula* spontaneamente trasmessi, per l'eventuale instaurazione di un rapporto lavorativo.

Parallelamente muta anche la disciplina dell'obbligo di rendere l'informativa all'interessato. A tal fine si aggiunge, all'art. 13 del Codice, un nuovo comma 5-*bis*, che esclude l'obbligo di informativa preliminare al trattamento dei dati nel caso in cui il candidato abbia spontaneamente inviato il proprio *curriculum vitae* a un determinato soggetto (pubblico o privato), per l'eventuale "*instaurazione di un rapporto di lavoro*".

Si prevede tuttavia, in capo al titolare, l'obbligo di fornire all'interessato, al momento del primo contatto successivo all'invio del *curriculum*, un'informativa semplificata, che concerna tra l'altro, finalità e modalità del trattamento, ambito di comunicazione dei dati e soggetti suscettibili di venirne a conoscenza, in qualità di responsabili o incaricati, estremi identificativi del titolare (cfr. art. 13, comma 1, lett. *a*), *d*) ed *f*)).

Va al riguardo rilevato come gran parte di tali modifiche corrispondano a quanto il Garante aveva prescritto nel 2002 sul trattamento di dati personali contenuti in *curricula* spontaneamente trasmessi, con particolare riferimento all'esigenza di adempiere comunque agli obblighi dell'informativa –e di richiesta dell'eventuale consenso– ma solo in caso *"di successivo"* trattamento dei dati contenuti nei *curricula* ricevuti (cfr. provv. 10 gennaio 2002, [doc. *web* n. 1064553]).

2) Le comunicazioni "infragruppo"

L'art. 6, comma 2, lett. *a*), n. 3), del decreto legge, inserendo nel comma 1 dell'art. 24 del Codice la lett. i-*ter*), ha previsto un'esenzione dall'obbligo di acquisizione del consenso –ma non dall'applicazione delle restanti disposizioni del Codice (es. informativa, misure di sicurezza, ecc.)– in relazione alla comunicazione di dati personali che:

a) avvenga fra *"società, enti o associazioni"* con *"società controllanti, controllate o collegate ai sensi dell'art. 2359 del codice civile ovvero con società sottoposte a comune controllo"*, oppure fra "*consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti"*;

b) sia in ogni caso effettuata per *"finalità amministrativo contabili"*.

Secondo la relazione illustrativa del d.d.l. di conversione del decreto legge, si tratta di *"trattamenti effettuati sulla base di rapporti di controllo e di collegamento tra società e nell'ambito delle altre forme di organizzazione congiunta dell'attività d'impresa (consorzi, associazioni temporanee di imprese, joint venture, reti d'impresa eccetera). La finalità è di semplificare i trattamenti effettuati per le esigenze operative delle imprese, che hanno rapporti di controllo e di collegamento e che rappresentano una componente diffusa nel tessuto imprenditoriale italiano, nel rispetto di un attento bilanciamento degli interessi del titolare, del terzo destinatario e dell'interessato"*.

La norma suscita taluni dubbi interpretativi. In particolare, emerge, in relazione all'ambito soggettivo di applicazione, l'incongruità del riferimento a "enti" e "associazioni", non potendosi ipotizzare, in relazione a tali categorie soggettive, un rapporto di collegamento o controllo ai sensi dell'art. 2359 del codice civile, che riguarda come noto le sole società. Inoltre è poco chiaro, ancora in relazione all'ambito soggettivo di applicazione, se le comunicazioni ivi previste debbano intercorrere necessariamente tra ciascun soggetto collettivo ivi indicato (consorzi, reti di imprese e raggruppamenti e associazioni temporanee di imprese) e i soggetti aderenti al medesimo soggetto collettivo ovvero anche nell'ambito degli stessi enti collettivi (ad esempio fra due imprese della stessa rete). La *ratio* della norma –volta a semplificare "*i trattamenti effettuati per le esigenze operative delle imprese*"– indurrebbe a preferire la seconda soluzione, che pure amplia di molto l'ambito applicativo della norma di esenzione.

Inoltre, si rileva che una clausola di salvaguardia relativa all'art. 130 del Codice sembra dettata per sottrarre espressamente all'applicazione della norma di esonero i trattamenti effettuati per fini promozionali o pubblicitari, anche se per ciò dovrebbe

essere sufficiente il richiamo alla necessaria finalizzazione del trattamento a scopi amministrativo-contabili.

Va poi verificata la portata della norma nella parte in cui stabilisce che l'esonero del consenso opera *"purché"* le finalità amministrativo-contabili perseguite *"siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'art. 13"*. La norma rimette dunque all'iniziativa del titolare del trattamento l'individuazione, in concreto, delle finalità amministrativo-contabili cui è preordinato il trattamento; individuazione che costituisce, dunque, condizione di legittimità del trattamento stesso, effettuato in assenza del consenso dell'interessato. In proposito va ricordato che già l'art. 13 medesimo prevede inderogabilmente l'obbligo di informare l'interessato circa *"le finalità ... del trattamento cui sono destinati i dati"*.

Si osserva, inoltre, che l'esonero dall'acquisizione del consenso non è richiamato con riferimento ai trasferimenti "infragruppo" verso Paesi terzi, per i quali permangono dunque gli obblighi relativi all'acquisizione del consenso o all'applicazione delle altre disposizioni di cui agli artt. 43 e 44 del Codice (es. clausole contrattuali tipo), creando così un regime differenziato a seconda che la comunicazione di dati personali avvenga o meno all'interno dei confini nazionali.

Infine, la portata applicativa della norma in esame è condizionata dall'interpretazione del concetto di "finalità amministrativo-contabili". La definizione di tale nozione (*recte*: dei trattamenti effettuati per le suddette finalità) era stata inserita dallo stesso d.l. n. 70/2011 al comma 1-*ter* dell'art. 34 del Codice (su cui v. *infra)* con una valenza inizialmente più ampia dell'attuale, in quanto costituente elemento integrativo anche di altre fattispecie la cui disciplina è nel frattempo mutata (per quanto concerne, in particolare, le misure di sicurezza, cfr. il paragrafo successivo).

Da un lato la definizione dei trattamenti effettuati per finalità amministrativo-contabili si riferisce ai trattamenti "connessi" allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile. Dall'altro lato, tuttavia –come può evincersi dalla seconda parte della disposizione– sembra attribuirsi *ipso iure* tale finalità ad un'ampia platea di "attività" ("*attività organizzative interne, quelle funzionali*

all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale - assistenziale, di salute, igiene e sicurezza sul lavoro") che, di per sé, invece, non sono soltanto funzionali ai correnti adempimenti amministrativi e contabili di un'impresa, ma attengono invece ai servizi stessi da essa resi o ad adempimenti e obblighi previsti dalla legge e, in quanto tali, non dovrebbero rientrare nell'ambito applicativo della norma e quindi, dell'"esenzione" in parola (si pensi all'attività precontrattuale o contrattuale, all'applicazione delle norme sindacali o sulla sicurezza del lavoro). Viceversa, sono semmai le attività amministrativo-contabili, in talune ipotesi, funzionali alle altre attività, anche organizzative, svolte dall'impresa o dall'ente per il perseguimento delle proprie finalità.

In linea generale, la definizione –già di per sé notevolmente ampia– abbraccia una serie potenzialmente indefinita di casi, dal momento che l'elencazione delle attività cui sono connessi i trattamenti "esentati" è meramente esemplificativa, come può evincersi dall'apertura del secondo periodo del comma 1-*ter* ("*In particolare, perseguono tali finalità le attività…*"). Ne consegue, ancora una volta, come l'ambito di applicazione della disciplina differenziata delle comunicazioni di dati "infragruppo" di cui all'art. 24, comma 1, lett. i-*ter)* del Codice non sia esattamente determinabile, in ragione dei dubbi interpretativi che la norma suscita.

2.1.3. Misure di sicurezza

Relativamente alla disciplina delle misure di sicurezza, durante il periodo di riferimento si sono susseguite importanti novelle al Codice, con particolare riferimento all'obbligo di adozione del documento programmatico sulla sicurezza (dps).

In un primo momento, infatti, l'art. 6, comma 2, lett. *a*), n. 5, del d.l. n. 70/2011, nel novellare il comma 1-*bis*, dell'art. 34 del Codice, aveva, tra l'altro, esteso la possibilità (già prevista dal d.l. n. 112/2008) di sostituzione del dps con l'autocertificazione ai soggetti che trattassero con strumenti elettronici soltanto dati personali non sensibili e come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori (anche se

"extracomunitari" o si tratti del coniuge o di parenti). Il contenuto dell'autocertificazione concerneva le sole misure *minime,* previste dal Codice e dall'Allegato B. Ciò non esonerava, ovviamente, i titolari dall'adottare anche le misure di sicurezza "adeguate" previste, in generale, dall'art. 31 del Codice.

Con il d.l. 9 febbraio 2012, n. 5, (cd. "decreto semplifica-Italia") l'obbligo di tenuta del dps e, conseguentemente, la facoltà di sostituzione dello stesso con l'autocertificazione sono stati invece soppressi (art. 45, comma 1, lett. *c*)). Inoltre, è venuto meno anche il predetto potere del Garante di individuare con proprio provvedimento modalità semplificate di applicazione delle misure minime di sicurezza per i trattamenti effettuati per correnti finalità "amministrativo-contabili", previsto anch'esso dal comma 1-*bis,* dell'art. 34, che è stato integralmente abrogato.

2.1.4. Dati giudiziari

L'art. 45, comma 1, lett. *a*) e *b*), del citato decreto legge "semplifica-Italia" consente il trattamento di dati giudiziari in attuazione di protocolli di intesa stipulati con il Ministero dell'interno o con i suoi uffici periferici, che specifichino la tipologia dei dati trattati e delle operazioni eseguibili. In relazione a tale norma, il Garante aveva fornito al Parlamento durante l'esame in prima lettura del disegno di legge di conversione, talune osservazioni volte al perfezionamento della disciplina in esame.

In primo luogo, il Garante rilevava l'esigenza di indicare in maniera maggiormente precisa le finalità per il perseguimento delle quali si autorizza il trattamento di dati giudiziari. Infatti, tale scopo è indicato solo *per relationem,* con riferimento cioè alle finalità sottese non già al trattamento dei dati, ma ai protocolli d'intesa *"in attuazione dei quali"* il trattamento stesso è effettuato. Peraltro, la nozione di *"prevenzione e (...) contrasto dei fenomeni di criminalità organizzata"* non circoscrive con precisione le finalità per il perseguimento delle quali si legittima il trattamento dei dati. Non solo, infatti, si fa riferimento a una nozione, quale quella di *"criminalità organizzata"*, che non ha una definizione giuridica propria, ma, di più, il trattamento viene autorizzato per *"la prevenzione e il contrasto"* dei suddetti fenomeni, dunque per attività indicate, anch'esse, in maniera generica.

Inoltre, una più precisa indicazione delle finalità per le quali il trattamento è autorizzato *ex lege* avrebbe contribuito anche –ad avviso del Garante– ad evidenziare il nesso che necessariamente deve sussistere tra lo specifico protocollo stipulato, lo scopo cui esso è preordinato e i soggetti, pubblici e privati, legittimati al trattamento, anche al fine di impedire utilizzazioni abusive di dati personali così delicati e perciò meritevoli di una tutela particolare. In secondo luogo, il Garante manifestava forti perplessità in ordine alla scelta di demandare la definizione della tipologia dei dati trattati e delle operazioni eseguibili ad atti –quali i protocolli d'intesa– che hanno natura convenzionale, non normativa e comunque non sono equiparabili alle fonti legittimate, ai sensi degli artt. 21 e 27 del Codice, a disciplinare tali aspetti (la stessa legge, il provvedimento del Garante o, per il trattamento effettuato da soggetti pubblici, il regolamento).

Sarebbe stato pertanto preferibile, ad avviso del Garante, demandare la definizione della tipologia dei dati trattati e delle operazioni eseguibili ad un atto di natura regolamentare –previa acquisizione del parere del Garante– cui i protocolli d'intesa avrebbero dovuto poi conformarsi. In ogni caso, al fine di elevare le garanzie del diritto alla protezione dei dati personali, il Garante sottolineava l'opportunità di prevedere il proprio parere conforme in ordine ai protocolli d'intesa stipulati (da soggetti pubblici e privati) con il Ministero dell'interno e destinati a disciplinare in concreto le modalità del trattamento dei dati.

2.1.5. Marketing postale

Come evidenziato nella citata audizione del 1° giugno 2011, nel novellare il comma 3-*bis* dell'art. 130 del Codice (comma aggiunto dall'art. 20-*bis*, del d.l. 25 settembre 2009, n. 135, cd. "decreto Ronchi", nel testo integrato dalla relativa legge di conversione), il d.l. n. 70/2011 ha esteso al *marketing* postale la disciplina introdotta in materia di *telemarketing* e di opposizione mediante iscrizione nell'apposito registro pubblico (cd. "*opt-out*"); ciò parrebbe rendere necessario una corrispondente modifica del regolamento attuativo, calibrato sul solo *marketing* telefonico. In sintesi, in virtù della suddetta novella, sarà possibile utilizzare gli indirizzi contenuti negli elenchi telefonici pubblici per effettuare, mediante comunicazioni cartacee, attività promozionali, salvo che il destinatario abbia esercitato il proprio diritto di opposizione, iscrivendosi nell'apposito registro.

Va sul punto rilevato, tuttavia, che la disciplina del trattamento di dati personali per finalità di *marketing* postale era già stata ampiamente semplificata, in particolare mediante il provvedimento del Garante del 19 giugno 2008 [doc. *web* n. 1526724], che ha introdotto un'ulteriore deroga al principio del consenso, prevedendo il regime del cd. "*soft-spam*" (già previsto per la posta elettronica dall'art. 130, comma 4, del Codice) anche nell'ambito della posta cartacea. Pertanto, l'estensione del regime dell'*opt-out* al *marketing* postale, nei termini sopra descritti, che interviene sul delicato equilibrio raggiunto fra tutela della riservatezza e ragioni del mercato, parrebbe alterare la finalità per la quale gli elenchi telefonici sono formati, in sostanziale disarmonia con il quadro normativo.

2.1.6. Norme processuali

Il d.lgs. 1° settembre 2011, n. 150, recante "Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione" (sul cui schema il Garante ha reso parere, cfr. paragrafo 1.2.4.), ha introdotto talune modifiche al procedimento relativo all'applicazione delle disposizioni del Codice.

In particolare, il provvedimento, nel ricondurre –in ossequio al criterio di delega di cui all'art. 54, comma 4, lett. *b*), n. 1, della l. 18 giugno 2009, n. 69– i procedimenti in cui sono prevalenti caratteri di *"concentrazione processuale, ovvero di officiosità dell'istruzione"* al rito del lavoro, ha annoverato fra questi anche il procedimento relativo all'applicazione delle disposizioni del Codice in materia di protezione dei dati personali.

Segnatamente, l'art. 10 prevede, al comma 1, che, ove non diversamente disposto dallo stesso articolo, le controversie di cui all'art. 152 del Codice siano regolate dal rito del lavoro. I commi successivi dell'art. 10 recano norme procedurali specifiche, che riproducono sostanzialmente quelle previgenti, in particolare in materia di: competenza territoriale; termine per la proposizione del ricorso avverso i provvedimenti del Garante; condizioni per la sospensione dell'efficacia esecutiva del provvedimento impugnato; eventuale estinzione del processo per mancata comparsa del ricorrente che non adduca alcun impedimento legittimo; inappellabilità della sentenza che definisce il giudizio e sua idoneità a prescrivere le misure necessarie anche in deroga al divieto di cui all'art. 4, della l. 20 marzo 1865, n. 2248, Allegato E).

L'art. 34, comma 9, del decreto abroga quindi i commi da 2 a 14 dell'art. 152 del Codice e vi inserisce invece un comma 1-*bis* che detta una norma di rinvio all'art. 10 del decreto stesso, quale fonte di disciplina della procedura giurisdizionale relativa alle controversie di cui al comma 1 dell'art. 152, e dunque a *"tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni"* del Codice, *"comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione"*, nonché alle *"controversie previste dall'art. 10, comma 5, della l. 1° aprile 1981, n. 121"*. Tale ultimo periodo è stato aggiunto dal decreto per confermare che la medesima disciplina processuale prevista per le controversie inerenti all'applicazione delle norme del Codice si estende anche alle controversie relative al diritto di accesso a dati conservati nel CED interforze del Dipartimento della pubblica sicurezza, ai sensi del previgente comma 14 dell'art. 152 del Codice.

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

Nel 2011 sono stati approvati alcuni provvedimenti normativi che hanno riguardato il trattamento dei dati personali e l'attività del Garante.

Vanno ricordati (oltre quelli già menzionati nella Relazione 2010, p. 25 ss.), in particolare:

Comunicazioni elettroniche

– la l. 15 dicembre 2011, n. 217, recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2010".

Per quanto di specifico interesse dell'Autorità, una norma di delega reca i princìpi e criteri direttivi per l'attuazione delle Direttive del Parlamento europeo e del Consiglio n. 2009/136/CE del 25 novembre 2009 e n. 2009/140/CE del 25 novembre 2009, in materia di comunicazioni elettroniche (art. 9). La prima direttiva modifica la Direttiva n. 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, la Direttiva n. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e il Regolamento del Parlamento europeo e del Consiglio n. 2006/2004 del 27 ottobre 2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori.

I decreti legislativi dovranno essere adottati attraverso l'adeguamento e l'integrazione delle disposizioni legislative in materia, tra le quali rientra il Codice (art. 9, comma 2).

Nell'ambito dei criteri di delega individuati sono di particolare interesse per l'Autorità i seguenti:

a) rispetto dei diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 e ratificata dalla l. 4 agosto 1955, n. 848, nell'alveo dei procedimenti restrittivi dell'accesso alle reti di comunicazione elettronica (art. 9, comma 4, lett. *b*));

b) rafforzamento delle prescrizioni in tema di sicurezza e riservatezza delle comunicazioni, nonché di protezione dei dati personali e delle informazioni già archiviate nell'apparecchiatura terminale, fornendo all'utente indicazioni chiare e comprensibili circa le modalità di espressione del proprio consenso, in particolare mediante le opzioni dei programmi per la navigazione nella rete internet o altre applicazioni (lett. *i*));

c) individuazione, per i rispettivi profili di competenza, del Garante per la protezione dei dati personali e della Direzione nazionale antimafia quali autorità nazionali ai fini dell'art. 15, paragrafo 1-*ter*, della citata Direttiva n. 2002/58/CE (lett. *l*));

d) definizione del riparto di attribuzioni tra Autorità per le garanzie nelle comunicazioni e Garante per la protezione dei dati personali, nell'adempimento delle funzioni previste dalle direttive, nel rispetto del quadro istituzionale e delle funzioni e dei compiti del Ministero dello sviluppo economico, fatta salva la competenza generale della Presidenza del Consiglio dei ministri in materia di diritto d'autore sulle reti di comunicazione elettronica e quella del Ministero per i beni e le attività culturali (lett. *q*));

e) revisione delle sanzioni e degli illeciti, con la previsione di sanzioni amministrative in caso di violazione delle norme introdotte dall'art. 2 della citata Direttiva n. 2009/136/CE e con il conseguente riassetto del sistema sanzionatorio disciplinato, in particolare, dal Codice, anche mediante depenalizzazione (lett. *r*)).

– Il decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, recante "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici" (cd. "salva-Italia"), con riferimento al quale si segnala:

a) a parte l'art. 40, comma 2, modificativo del Codice (per il quale vedi par. 2.1.1.), è di particolare interesse l'art. 11 (commi da 2 a 4-*bis*) in base al quale gli operatori

Contrasto dell'evasione fiscale

finanziari sono obbligati a comunicare periodicamente all'Anagrafe tributaria le movimentazioni che hanno interessato i rapporti finanziari con la clientela (di cui all'art. 7, sesto comma, del d.P.R. 29 settembre 1973, n. 605) ed ogni informazione relativa ai predetti rapporti necessaria ai fini dei controlli fiscali, nonché l'importo delle operazioni finanziarie indicate nella predetta disposizione. Con provvedimento del Direttore dell'Agenzia delle entrate sono stabilite le modalità della comunicazione, estendendo l'obbligo di comunicazione anche ad ulteriori informazioni relative ai rapporti strettamente necessarie ai fini dei controlli fiscali. Le predette informazioni sono utilizzate dall'Agenzia delle entrate anche per l'elaborazione con procedure centralizzate, secondo i criteri individuati con provvedimento del Direttore della medesima Agenzia, di specifiche liste selettive di contribuenti a maggior rischio di evasione. In proposito, nel corso dei lavori parlamentari, il Garante, con una lettera inviata al Presidente della Commissione finanze della Camera dei deputati, ha rilevato che la norma in questione solleva numerose perplessità sul rispetto dei princìpi di necessità e di proporzionalità, in particolare per quanto riguarda l'ingente numero di dati che gli operatori finanziari devono trasmettere all'Anagrafe tributaria. La disposizione prevede, infatti, che ad essa siano trasferiti i dati relativi alle operazioni finanziarie di tutti i clienti degli intermediari finanziari. Il Garante ha inoltre espresso perplessità sulla previsione relativa al potere del Direttore dell'Agenzia delle entrate di ampliare ulteriormente, con proprio provvedimento, la tipologia e il numero dei dati da trasferire. Si tratta infatti, in questo caso, di una vera e propria "norma in bianco", che attribuisce a un'autorità amministrativa il potere di imporre la comunicazione di dati personali senza vincoli né parametri che non siano quelli relativi a un generale richiamo alla lotta all'evasione fiscale. L'Autorità ha concluso la segnalazione auspicando un perfezionamento della norma con specificazioni indispensabili ai fini del rispetto del principio di legalità del trattamento dei dati personali. In ogni caso l'Autorità ha richiesto che il provvedimento dell'Agenzia delle entrate disciplini anche le misure di sicurezza e l'accesso selettivo ai dati, previo parere del Garante. Secondo un'altra norma di interesse, l'Inps è tenuta a fornire all'Agenzia delle entrate ed alla

Guardia di finanza i dati relativi alle posizioni di soggetti destinatari di prestazioni socio-assistenziali affinché vengano considerati ai fini della effettuazione di controlli sulla fedeltà dei redditi dichiarati, basati su specifiche analisi del rischio di evasione (art. 11, comma 6);

b) con d.P.C.m. dovranno essere ridefinite le modalità di determinazione del sistema dei controlli dell'ISEE, prevedendo, tra l'altro, la costituzione di una banca dati delle prestazioni sociali agevolate, condizionate all'ISEE, attraverso l'invio telematico all'Inps, da parte degli enti erogatori, nel rispetto del Codice, delle informazioni sui beneficiari e sulle prestazioni concesse (art. 5); ISEE

c) infine, allo scopo di perseguire il contenimento della spesa complessiva per il funzionamento delle autorità amministrative indipendenti, è prevista una riduzione del numero dei componenti di alcune di esse (Autorità per le garanzie nelle comunicazioni; Autorità per la vigilanza sui contratti pubblici di lavori; servizi e forniture, Autorità per l'energia elettrica e il gas; Autorità garante della concorrenza e del mercato; Commissione nazionale per la società e la borsa; Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo; Commissione per la vigilanza sui fondi pensione; Commissione per la valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche; Commissione di garanzia dell'attuazione della legge sullo sciopero nei servizi pubblici essenziali). La norma precisa che qualora il numero dei componenti, incluso il Presidente, risulti pari, ai fini delle deliberazioni, in caso di parità, il voto del Presidente vale doppio. Da ultimo (art. 23) si stabilisce che il Presidente e i componenti degli organismi citati e delle altre autorità amministrative indipendenti di cui all'elenco Istat previsto dall'art. 1, comma 3, della l. 31 dicembre 2009, n. 196, non possono essere confermati alla cessazione dalla carica. Riduzione dei costi delle autorità indipendenti

– La l. 12 novembre 2011, n. 183, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato. (Legge di stabilità 2012)". Il provvedimento prevede alcune disposizioni d'interesse per l'Autorità, di seguito brevemente illustrate:

a) l'art. 4 stabilisce che al personale delle amministrazioni pubbliche di cui all'elenco Istat sopra citato, che si trovi in posizione di comando, distacco o altra analoga situazione Riduzione della spesa pubblica

presso le autorità indipendenti non è possibile erogare, da parte di queste ultime, indennità, compensi o altri emolumenti finalizzati ad operare perequazioni rispetto al trattamento economico fondamentale più elevato corrisposto al personale dei rispettivi ruoli (comma 48). La disposizione in questione è applicabile anche alle indennità, compensi o altri emolumenti già in godimento al 1° gennaio 2012; eventuali clausole difformi contenute nei regolamenti delle autorità indipendenti sono disapplicate (comma 49). La norma va ora applicata anche alla luce di quanto disposto dall'art. 23-*ter*, comma 1, del d.l. 6 dicembre 2011, n. 201 (cd. "decreto salva-Italia") il quale individua un parametro limite per le somme che possono essere corrisposte ai dipendenti delle pubbliche amministrazioni che siano chiamati a svolgere funzioni direttive dirigenziali o equiparate, anche in posizione di fuori ruolo o di aspettativa, presso ministeri o enti pubblici nazionali, comprese le autorità amministrative indipendenti. In particolare, la disposizione prevede che questi soggetti –se conservano il trattamento economico riconosciuto dall'amministrazione di appartenenza– non possano ricevere a titolo di retribuzione, indennità, o anche solo per il rimborso spese, più del 25% dell'ammontare complessivo del trattamento economico già percepito. Per completezza, si segnala che in base al medesimo art. 23-*ter*, con d.P.C.m. dovrà essere definito il trattamento economico di chiunque riceva emolumenti o retribuzioni dalle pubbliche amministrazioni, nel rispetto di un parametro massimo e salvo espresse deroghe motivate al tetto delle retribuzioni, per coloro che siano chiamati a ricoprire posizioni apicali nell'amministrazione;

Semplificazione dei pagamenti e degli accertamenti delle violazioni all'obbligo di copertura assicurativa

b) l'art. 13, nel novellare l'art. 193 del nuovo codice della strada (d.lgs. 30 aprile 1992, n. 285), dispone, in particolare, che la verifica sulla copertura assicurativa obbligatoria possa essere effettuata anche attraverso il confronto tra dati relativi alle polizze emesse dalle imprese assicuratrici con quelli provenienti dai dispositivi o apparecchiature omologati o approvati per il funzionamento in modo completamente automatico e gestiti direttamente dagli organi di polizia stradale (art. 193, comma 4-*ter*). In modo speculare si prevede, altresì, che la documentazione fotografica prodotta dai predetti dispositivi o apparecchiature costituisce atto di accertamento ai sensi dell'art. 13 della l. 24 novembre 1981, n. 689 (art. 193, comma 4-*quinquies*);

Modifiche in materia di documentazione amministrativa

c) l'art. 15 prevede una serie di modifiche al d.P.R. 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. In particolare, il nuovo art. 40 del testo unico dispone che le certificazioni della pubblica amministrazione in ordine a stati, qualità personali e fatti sono valide solo nei rapporti tra privati, mentre nei rapporti con la pubblica amministrazione i certificati e gli atti di notorietà sono sempre sostituiti dalle dichiarazioni sostitutive. Inoltre, con una novella al comma 1 dell'art. 43, si sancisce, in capo ad amministrazioni pubbliche e gestori di pubblici servizi, l'obbligo di acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive di cui agli artt. 46 e 47 ovvero di accettare la dichiarazione sostitutiva prodotta dall'interessato. Al riguardo, il novellato art. 72 ("Responsabilità in materia di accertamento d'ufficio e di esecuzione dei controlli") stabilisce che, ai fini, in particolare, dell'accertamento d'ufficio di cui all'art. 43, le amministrazioni certificanti individuano un ufficio responsabile, rendendo note, con pubblicazione sul sito istituzionale, le misure organizzative adottate;

Impiego della PEC nel processo civile

d) l'art. 25 reca, al comma 1, talune modifiche al codice di procedura civile, sopprimendo, in particolare, l'obbligo –recentemente introdotto dal d.l. n. 138/2011– di effettuare le comunicazioni di cancelleria alle parti esclusivamente tramite PEC o telefax e riscrivendo la disciplina delle comunicazioni di cancelleria. Secondo la nuova norma, dunque, le comunicazioni di cancelleria si effettuano in via ordinaria tramite consegna al destinatario, che rilascia ricevuta, o tramite PEC, nel rispetto della vigente normativa, anche regolamentare, sui documenti informatici. Se non è possibile procedere con questi mezzi, la comunicazione avviene tramite telefax o tramite notifica dell'ufficiale giudiziario, salva diversa disposizione di legge (art. 136 c.p.c., come modificato dalla lett. *d)* del predetto comma). Il comma 2 dell'art. 25, nel novellare le disposizioni di attuazione del codice di procedura civile relative all'espropriazione immobiliare, elegge a modalità preferenziale di comunicazione della relazione di stima dell'esperto, nonché della presentazione delle offerte di acquisto e della presentazione della cauzione, la comunicazione tramite PEC. Il comma 3, nel novellare la l. n. 53/1994, estende a tutti gli atti in materia civile, amministrativa e stragiudiziale la possibilità di notificazione mediante PEC.

– Il decreto legge 13 agosto 2011, n. 138, convertito, con modificazioni, dalla l. 14 settembre 2011, n. 148, recante ulteriori misure urgenti per la stabilizzazione finanziaria e per lo sviluppo.

Accertamenti tributari dei comuni

a) Nell'ambito del rafforzamento degli strumenti a disposizione dei comuni ai fini dell'accertamento tributario, si prevede che con decreto siano individuati ulteriori dati che l'Agenzia delle entrate deve mettere a disposizione dei comuni e dei consigli tributari per favorire la partecipazione all'attività di accertamento, nonché le modalità di trasmissione idonee a garantire la necessaria riservatezza (art. 1, comma 12-*ter*, lett. *e*));

Accesso ai sistemi informativi

b) si prevede che ai sistemi informativi di cui all'art. 117 del Codice a fini di concessione di crediti al consumo (cd. "Sic - Sistemi di informazioni creditizie") possano avere accesso, anche per le finalità ivi previste, i soggetti che partecipano al sistema di prevenzione antifrode di cui al comma 5, dell'art. 30-*ter* del d.lgs. 13 agosto 2010, n. 141 (ovvero banche, intermediari finanziari, fornitori di servizi di comunicazione elettronica ecc.), fatta salva la facoltà di istituire e partecipare ai sistemi di cui all'art. 119 del Codice sui dati relativi al comportamento debitorio nei casi diversi da quelli di cui all'art.117 (art. 6-*bis*).

Tecnologie dell'informazione nella giustizia tributaria

– Il d.l. 6 luglio 2011, n. 98, convertito, con modificazioni, dalla l. 15 luglio 2011, n. 111, recante disposizioni urgenti per la stabilizzazione finanziaria. Di interesse è l'art. 39, comma 8, in base al quale ai fini dell'attuazione dei princìpi previsti dal codice dell'amministrazione digitale nella materia della giustizia tributaria nonché per assicurare l'efficienza e la celerità del relativo processo, con regolamento emanato dal Ministero dell'economia e delle finanze, sentito anche il Garante, sono introdotte disposizioni per l'adeguamento del processo tributario alle tecnologie dell'informazione e della comunicazione, in attuazione dei princìpi previsti dal medesimo codice dell'amministrazione digitale.

– Il decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla l. 12 luglio 2011, n. 106, recante prime disposizioni urgenti per l'economia. Oltre alle disposizioni modificative del Codice (per le quali vedi par. 2.1.), si segnalano:

Costruzione delle opere pubbliche

a) l'art. 4 che introduce una serie di modifiche alla disciplina vigente al fine, tra l'altro, di semplificare le procedure di affidamento dei contratti pubblici; in particolare, in base

alla lett. *i*) del comma 1, l'individuazione, l'accertamento e la prova dei requisiti di partecipazione alle gare devono avvenire mediante collegamento telematico alla banca dati nazionale dei contratti pubblici;

Costruzioni private

b) l'art. 5, il cui comma 1 apporta modificazioni alla disciplina vigente al fine di liberalizzare le costruzioni private; in particolare, la lett. *d*) prevede che l'obbligo di comunicazione all'autorità locale di pubblica sicurezza sia assorbito dalla registrazione dei contratti di trasferimento immobiliare. Inoltre, il comma 4-*bis* per agevolare la circolazione delle informazioni concernenti gli immobili, abolisce il divieto di riutilizzazione commerciale dei dati ipotecari e catastali, consentendo il riutilizzo dei documenti, dei dati e delle informazioni catastali e ipotecari a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i documenti sono stati prodotti, fermo restando il rispetto della normativa in materia di protezione dei dati personali;

Semplificazioni degli adempimenti burocratici

c) l'art. 6, che al fine di ridurre gli oneri normativi, in particolare per le piccole e medie imprese, prevede una serie di novità tra cui: 1) quella relativa alle pubbliche amministrazioni che *"devono pubblicare sul proprio sito istituzionale l'elenco degli atti e documenti necessari per ottenere provvedimenti amministrativi"* (lett. *b*)); 2) quella relativa alla facoltà di effettuare *online* qualunque transazione finanziaria Asl-imprese e cittadini (lett. *d*)); in attuazione di tale norma, il comma 2, lett. *d*), dello stesso articolo, reca disposizioni rivolte ad *"accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini, riducendone i costi connessi"*. Al riguardo, ai sensi del codice dell'amministrazione digitale, le Asl adottano procedure telematiche per consentire il pagamento *online* delle prestazioni erogate, nonché la consegna tramite modalità digitali (*web*, posta elettronica certificata ecc.) dei referti medici, salvo il diritto dell'interessato di ottenere copia cartacea del referto redatto in forma elettronica (punto 1). Le disposizioni attuative sono adottate con decreto del Presidente del Consiglio dei ministri, previo parere del Garante, entro novanta giorni dall'entrata in vigore della legge di conversione del decreto (punto 2); 3) infine, nel perseguimento dell'obiettivo di riduzione degli oneri amministrativi definito in sede di Unione

europea, si estende la misurazione degli oneri amministrativi ai settori regolati dalle autorità amministrative indipendenti; a tal proposito, *"le autorità amministrative indipendenti di vigilanza e garanzia effettuano, nell'ambito dei propri ordinamenti, la misurazione degli oneri amministrativi a carico delle imprese con l'obiettivo di ridurre tali oneri entro il 31 dicembre 2012, proponendo le misure legislative e regolamentari ritenute idonee a realizzare tale riduzione"* (comma 3);

Semplificazione fiscale

d) l'art. 7 prevede modifiche alla disciplina vigente per ridurre il peso della burocrazia che grava sulle imprese e più in generale sui contribuenti. In particolare, si prevede che una serie di atti siano adottati senza richiedere informazioni già disponibili nei sistemi informativi, evitandone, conseguentemente, la duplicazione. Inoltre, le Agenzie fiscali, gli enti di previdenza e assistenza obbligatoria e il Ministero del lavoro e delle politiche sociali possono stipulare apposite convenzioni con le amministrazioni pubbliche nonché con gli enti pubblici economici e con le autorità amministrative indipendenti, per acquisire, in via telematica, nel rispetto dei princìpi di cui agli artt. 20, commi 2 e 4, e 22 del Codice, dati e informazioni (anche in forma disaggregata) detenuti per obblighi istituzionali, utili al fine di ridurre gli adempimenti dei cittadini e delle imprese, e garantire una più efficace azione di contrasto alle evasioni e alle frodi, nonché per accertare il diritto e la misura delle prestazioni previdenziali, assistenziali e di sostegno al reddito; nella convenzione sono indicati i motivi per i quali si richiedono necessariamente i predetti dati ed informazioni. L'omessa fornitura dei dati è valutabile ai fini della responsabilità disciplinare e contabile del funzionario;

Segnalazioni dei ritardi di pagamento

e) l'art. 8-*bis* in materia di Sic (Sistemi di informazioni creditizie) –successivamente modificato dal d.l. 13 agosto 2011, n. 138, convertito, con modificazioni, dalla l. 14 settembre 2011, n. 148– in base al quale entro dieci giorni dalla regolarizzazione dei pagamenti, le segnalazioni relative a ritardi di pagamenti da parte delle persone fisiche o giuridiche già inserite nelle banche dati devono essere integrate dalla comunicazione dell'avvenuto pagamento, del quale l'istituto di credito deve dare notizia senza indugio;

Servizi ai cittadini

f) l'art. 10 volto a incentivare l'uso degli strumenti elettronici per aumentare l'efficienza nell'erogazione dei servizi ai cittadini e, in particolare, semplificare il procedimento di

rilascio dei documenti obbligatori di identificazione. Esso prevede che l'emissione della carta di identità elettronica sia riservata al Ministero dell'interno (comma 1), che con apposito decreto interministeriale definisce le modalità tecniche di attuazione (comma 2). Anche progressivamente la carta di identità elettronica sarà unificata attraverso un decreto del Presidente del Consiglio dei ministri con la tessera sanitaria, in modo da consentire il rilascio gratuito di un documento unificato (comma 3).

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

Banca dati nazionale unica della documentazione antimafia

- il d.lgs. 6 settembre 2011, n. 159, recante "Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136". Si prevede l'istituzione della banca dati nazionale unica della documentazione antimafia presso il Ministero dell'interno (art. 96), specificando i dati in essa contenuti (art. 98) e i soggetti legittimati alla consultazione (art. 97). Le modalità di funzionamento della stessa sono demandate ad un regolamento, da adottarsi previo parere del Garante (art. 99);

Controversie in materia di trattamento dei dati

- il d.lgs. 1° settembre 2011, n. 150, recante "Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione, ai sensi dell'art. 54 della legge 18 giugno 2009, n. 69" (vedi par. 2.1.6.);

Sistemi informativi e statistici della sanità

- il d.lgs. 23 giugno 2011, n. 118, recante "Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli artt. 1 e 2 della l. 5 maggio 2009, n. 42". In particolare, al fine di migliorare i sistemi informativi e statistici della sanità e per il loro migliore utilizzo in termini di monitoraggio dell'organizzazione dei livelli di assistenza, l'art. 35 prevede procedure di anonimizzazione dei dati individuali presenti nei flussi informativi, con la trasformazione del codice fiscale, ai fini di ricerca per scopi di statistica sanitaria, in codice anonimo, mediante apposito algoritmo biunivoco, in modo da tutelare l'identità dell'assistito nel procedimento di elaborazione dei dati;
- il d.lgs. 18 aprile 2011, n. 59, recante "Attuazione delle Direttive 2006/126/CE e 2009/113/CE concernenti la patente di guida". Si segnalano in particolare:

Idoneità alla guida

a) l'Art. 14, che, integrando l'art. 128 del codice della strada (con il comma 1-*quinquies*), ha esteso ad una più ampia categoria di medici l'obbligo informativo circa la sussistenza di patologie mediche suscettibili di incidere sulla idoneità alla guida, finora previsto solo a carico dei responsabili delle unità di terapia intensiva o di neurochirurgia per i casi di coma di durata superiore a 48 ore (art. 128, comma 1-*bis*, C.d.s., introdotto dalla recente l. 29 luglio 2010, n. 120). In base alla nuova disposizione, infatti, a decorrere dal 19 gennaio 2013, l'obbligo di comunicazione agli uffici provinciali del Dipartimento per i trasporti, la navigazione ed i sistemi informativi e statistici del Ministero delle infrastrutture e dei trasporti è esteso anche ai *"medici di cui all'art. 119, anche in sede di accertamenti medico legali diversi da quelli di cui al predetto articolo"* quando accertino, in soggetti già titolari di patente, la sussistenza di *"patologie incompatibili con l'idoneità alla guida ai sensi della normativa vigente"*. La formulazione della norma, decisamente ampia e non definita, richiama sostanzialmente a tale obbligo tutti i medici preposti all'accertamento dei requisiti fisici e psichici per il conseguimento della patente di guida, anche quando effettuano accertamenti medico-legali ad altri fini;

Patente elettronica

b) in conformità a quanto previsto dall'art. 1 della Direttiva n. 2006/126/CE, l'art. 22 prevede che, al fine di evitare rischi di falsificazione delle patenti di guida, previa adozione di apposite norme da parte della Commissione dell'Unione europea, lo Stato italiano possa inserire un supporto di memorizzazione (*microchip*) nelle patenti di guida contenente i dati armonizzati riportati nel modello allegato al decreto, *"fatte salve le norme relative alla protezione dei dati"*;

Requisiti fisici e psichici di idoneità alla guida

c) in attuazione dell'art. 7 della Direttiva n. 2006/126/CE, l'art. 23 stabilisce che l'accertamento dei requisiti fisici e psichici previsti dall'art. 119 del codice della strada per il conseguimento della patente di guida *"si conforma almeno ai requisiti minimi previsti dall'allegato III"*. Tale allegato ("Requisiti minimi di idoneità fisica e mentale per la guida di un veicolo a motore") annovera fra le patologie anche la "dipendenza da alcol o guida dipendente da alcol" e l'"uso di sostanze stupefacenti o psicotrope" e l'"abuso e consumo abituale di medicinali";

Prevenzione delle frodi nel settore del credito al consumo

– il d.lgs. 11 aprile 2011, n. 64, che mediante integrazione del d.lgs. 13 agosto 2010, n. 141, istituisce un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità. Il decreto è stato adottato in attuazione dell'art. 33, comma 1, lettere da d-*bis*) a d-*quinquies*), della l. 7 luglio 2009, n. 88 (legge comunitaria 2008), come integrato dalla legge comunitaria 2009 (l. 4 giugno 2010, n. 96) e riproduce sostanzialmente il testo di un disegno di legge ampiamente discusso in Parlamento e sul quale il Garante aveva, in più occasioni, espresso forti perplessità (audizioni del luglio 2008 e del novembre 2009, rispettivamente, presso le Commissioni finanze del Senato e della Camera dei deputati). In tali occasioni, l'Autorità aveva evidenziato uno "snaturamento" dell'originario impianto normativo e della configurazione del sistema, il quale, diversamente da quanto originariamente prospettato, non è più solo uno "snodo tecnico" attraverso il quale il gestore provvede a riscontrare le richieste di verifica provenienti dai soggetti aderenti al sistema su informazioni registrate in altre, distinte banche dati, ma assume, esso stesso, natura di vero e proprio archivio. Infatti, il sistema di prevenzione, istituito nell'ambito del Ministero dell'economia e delle finanze che è titolare del trattamento dei dati e gestito da Consap S.p.A. –responsabile del trattamento– risulta composto anche da un "modulo informatico di allerta" nel quale memorizzare le informazioni trasmesse dagli aderenti relative: a) alle frodi subite; b) ai casi che configurano un rischio di frode; c) agli allerta preventivi trasmessi dal titolare dell'archivio agli aderenti. Tali informazioni, peraltro, sono conservate nell'archivio per il tempo necessario ad accertare l'effettiva sussistenza del rischio di frodi (art. 30-*quater*, comma 1, lett. *c*), del d.lgs n. 141/2010, inserito dall'art. 1 del decreto). La previsione di tali flussi informativi è destinata a creare una banca dati di notevoli dimensioni, contenente informazioni di particolare delicatezza. Essa rischia, peraltro, di incoraggiare pericolose stigmatizzazioni dei cittadini che ricorrono al credito o ad altri servizi, sulla base di una valutazione rimessa agli stessi operatori del settore e non alle pubbliche autorità competenti in materia di prevenzione e repressione di comportamenti fraudolenti. Analoghe perplessità suscita, poi, la previsione di un servizio volto a ricevere segnalazioni da parte di soggetti che hanno subito o temono di aver subito frodi configuranti ipotesi di

furto di identità (art. 30-*ter*, comma 8, del d.lgs. n. 141/2010, inserito dall'art. 1 del decreto). Il decreto legislativo conferma, poi, la "partecipazione" al sistema da parte di categorie di soggetti per finalità non ben identificate o certamente diverse da quelle di valutazione del merito creditizio (ad es., "gestori di sistemi di informazioni creditizie"). Infine, contrariamente a quanto richiesto dal Garante nelle audizioni, il decreto prevede che ulteriori flussi di dati idonei a perseguire le finalità di contrasto delle frodi potranno essere individuati con il previsto decreto ministeriale di attuazione (art. 30-*quinquies*, comma 3, del d.lgs. n. 141/2010, inserito dall'art. 1 del decreto).

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

Registro delle sanzioni disciplinari del Coni

Nel 2011 il Garante ha espresso parere favorevole su due schemi di regolamento del Comitato olimpico nazionale italiano (Coni) riguardanti, rispettivamente, il "Registro delle sanzioni disciplinari" e le "Regole procedurali di carattere tecnico operativo per l'attuazione del Registro delle sanzioni disciplinari" (parere 16 febbraio 2011 [doc. *web* n. 1793469]).

Il primo schema è volto a disciplinare l'istituzione e la gestione del registro delle sanzioni disciplinari dell'ordinamento sportivo e le procedure di comunicazione, iscrizione, aggiornamento ed eliminazione dei dati utilizzati per verificare i requisiti di eleggibilità alle cariche elettive del Coni e degli altri organismi sportivi, nonché quelli della tesserabilità presso i medesimi organismi, così come previsto dall'ordinamento sportivo vigente. A tale fine, lo schema di regolamento prevede che nel registro gestito dal Coni, in qualità di titolare del trattamento, vengano iscritti per estratto dagli organismi sportivi e dagli organi di giustizia sportiva i provvedimenti sanzionatori, anche in materia di doping, quelli di clemenza, revisione, revocazione e riabilitazione, nonché i casi annotati in cui i tesserati si siano sottratti alle sanzioni irrogate nei loro confronti.

Il secondo schema di regolamento, invece, individua le regole tecniche di funzionamento del sistema informatico del registro, prevedendo l'implementazione di politiche di urezza idonee a salvaguardare la riservatezza, l'integrità, l'esattezza e la disponibilità delle informazioni e delle risorse del sistema.

Gli schemi di decreto hanno sostanzialmente recepito le indicazioni rese dall'Ufficio del Garante nel corso di vari contatti informali a livello tecnico, volti a garantire un più elevato *standard* di tutela del diritto alla protezione dei dati personali. In particolare, le predette indicazioni hanno riguardato l'esplicitazione delle finalità perseguite dai soggetti che hanno accesso al Registro, la gestione delle credenziali di autenticazione, la descrizione degli accorgimenti tecnici volti a garantire la sicurezza informatica dei dati ivi contenuti, nonché le

finalità e le modalità di accesso e utilizzo di un archivio storico delle transazioni intervenute sui provvedimenti iscrivibili nel Registro.

Unioncamere

Il Garante ha espresso parere favorevole sulla richiesta di Unioncamere di modifica della scheda, allegata allo schema tipo di regolamento per i trattamenti di dati sensibili e giudiziari effettuati dalle camere di commercio, che individua i tipi di dati e di operazioni eseguibili per le rilevanti finalità di interesse pubblico relative alla gestione e al rinnovo dei componenti degli organi collegiali di amministrazione e controllo (artt. 20, comma 2, 65 e 69 del Codice).

Tale modifica si è resa necessaria per l'entrata in vigore della nuova disciplina sulla composizione dei consigli camerali, contenuta nel d.lgs. 15 febbraio 2010, n. 23 e nei relativi decreti attuativi del 4 agosto 2011 nn. 155 e 156 (decreto in merito al quale il Garante ha espresso parere favorevole il 26 maggio 2011 [doc. *web* n. 1817531]). In particolare, le nuove procedure di designazione dei componenti dei consigli delle camere di commercio, introducono trattamenti di dati sensibili relativi agli iscritti alle organizzazioni di categoria, imprenditoriali e sindacali e agli associati alle associazioni dei consumatori contenuti negli elenchi che le stesse devono depositare presso la camera di commercio per la determinazione della rispettiva consistenza. Pertanto, qualora le camere di commercio modifichino i propri atti regolamentari in conformità a quanto previsto nella scheda valutata positivamente dal Garante, non devono richiedere all'Autorità un ulteriore parere specifico per trattare dati sensibili e giudiziari (parere 20 gennaio 2012 [doc. *web* n. 1870229]).

3.1.1. Regolamenti degli enti locali

Nell'anno di riferimento, si sono registrate alcune richieste di pareri degli enti locali relative 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 segnala la richiesta di un comune in merito alla necessità di introdurre nel proprio regolamento sui dati sensibili e giudiziari una nuova scheda, non prevista nel predetto schema tipo Anci, avente ad oggetto i trattamenti di dati personali derivanti dall'installazione di impianti di videosorveglianza. Al riguardo, è stato evidenziato che non occorre predisporre una scheda per i trattamenti di dati personali effettuati attraverso impianti audiovisivi, in quanto l'installazione di telecamere, nel caso rappresentato, non era preordinata al trattamento specifico di dati sensibili; i trattamenti in questione devono avvenire nel rispetto delle prescrizioni contenute nel Codice e delle indicazioni fornite dal Garante nel provvedimento in materia di videosorveglianza approvato l'8 aprile 2010 (in G.U. 29 aprile 2010, n. 99 [doc. *web* n. 1712680]) (nota 29 novembre 2011).

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

In ordine al primo profilo si menziona una segnalazione relativa alla pubblicazione sul bollettino ufficiale di una regione, accessibile anche dal sito internet istituzionale, delle graduatorie per la concessione di contributi per l'acquisto di attrezzature informatiche recanti l'indicazione delle generalità e del tipo di disabilità di cui erano affetti circa millenovecento persone. A seguito di un accertamento preliminare, è stato altresì verificato che le predette graduatorie erano accessibili a chiunque, attraverso una semplice ricerca nominativa dei beneficiari effettuata attraverso i comuni motori di ricerca. L'Ufficio, nel richiamare le indicazioni fornite nelle linee-guida del 2 marzo 2011 (cit. *infra*), relative alla pubblicazione di dati in internet da parte delle amministrazioni pubbliche, ha evidenziato che la disciplina sulla protezione dei dati personali vieta, in particolare, la diffusione di quelli idonei a rivelare lo stato di salute. A seguito dell'intervento del Garante, la regione ha provveduto a rimuovere dal sito *web* le graduatorie oggetto della segnalazione. Su tale base l'Ufficio, pur essendo stata riscontrata una condotta non conforme alla disciplina applicabile, non ha ravvisato i presupposti per

l'adozione di un provvedimento avente ad oggetto direttamente il trattamento dei dati, ma ha disposto gli opportuni accertamenti volti a verificare i presupposti per la contestazione, con un eventuale autonomo procedimento sanzionatorio, della violazione del divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (nota 3 novembre 2011).

Anche nel 2011 sono pervenute diverse richieste di chiarimento in ordine alle problematiche concernenti il trattamento dei dati personali connesso alla trasparenza dell'attività amministrativa e all'esercizio del diritto di accesso agli atti amministrativi ai sensi della l. 7 agosto 1990, n. 241.

In merito al secondo profilo, il Garante ha ribadito che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60), le quali attribuiscono il diritto di prendere visione e di estrarre copia di documenti amministrativi ai soggetti privati che abbiano un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso (artt. 22 e ss., l. 7 agosto 1990, n. 241, così come modificata dalla l. 11 febbraio 2005, n. 15; art. 2 d.P.R. 12 aprile 2006, n. 184).

Le valutazioni in ordine alle determinazioni dell'amministrazione interpellata in relazione a richieste di accesso ai documenti esulano dall'ambito di competenza del Garante, limitato alla protezione dei dati personali. Le scelte dell'amministrazione interpellata, in caso di ostensione dei documenti richiesti oppure di diniego dell'accesso, espresso o tacito, o di differimento dello stesso, rimangono sindacabili dinanzi al giudice amministrativo (art. 25, l. n. 241/1990 e ss.mm. citate) (nota 14 novembre 2011).

Analogamente, con specifico riferimento al diritto di accesso dei consiglieri comunali ad atti contenenti dati sensibili, è stato ricordato come l'esercizio di tale diritto, ai sensi dell'art. 65, comma 4, lett. *b)*, del Codice, è consentito laddove sia indispensabile allo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo (v. scheda n. 33 dello schema tipo Anci [doc. *web* n. 1174532] sul quale l'Autorità si era espressa positivamente il 21 settembre 2005 [doc. *web* n. 1170239]).

Spetta, pertanto, all'amministrazione destinataria della richiesta, senza richiedere alcun consenso agli interessati, né alcuna autorizzazione a questa Autorità, accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* del consigliere comunale e tale valutazione è eventualmente sindacabile dal giudice amministrativo (artt. 18, commi 2 e 4, 19, 59 e 60 del Codice).

Resta ovviamente ferma la necessità che i dati personali così acquisiti dagli aventi diritto siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, rispettando l'obbligo del segreto *"nei casi specificamente determinati dalla legge"*, nonché i divieti di divulgazione dei dati personali (si pensi ad esempio all'art. 22, comma 8, del Codice che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (nota 31 marzo 2011).

Quesiti specifici sono stati posti in ordine alle richieste di accesso di giornalisti dalle Regioni Piemonte, Toscana e Campania per la documentazione concernente i beneficiari e l'ammontare dei vitalizi percepiti dai consiglieri regionali cessati dal mandato, e dall'Ipab di Vicenza, dal Pio Albergo Trivulzio e dalla Provincia di Bologna in relazione all'elenco dei cittadini affittuari di immobili di proprietà pubblica. In merito, è stato rappresentato che qualora l'Amministrazione reputi legittima la richiesta di accesso rimane *"affidata alla responsabilità del giornalista l'utilizzazione lecita del dato raccolto e quindi la sua diffusione secondo i parametri dell'essenzialità rispetto al fatto d'interesse pubblico narrato, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo"*. Tale chiarimento –contenuto anche nel documento del Garante del 6 maggio 2004 [doc. *web* n. 1007634]– è rivolto a chi, nell'esercizio dell'attività giornalistica, utilizza la documentazione a cui ha avuto legittimamente accesso; esso costituisce un'applicazione dei princìpi generali già dettati dal Codice (cfr. in particolare art. 137) e dalle disposizioni del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (Allegato A.1. al Codice) (*ex plurimis*, note 20 aprile e 12 ottobre 2011).

Sono, inoltre, pervenute numerose istanze (segnalazioni, quesiti e richieste di parere) in ordine al corretto trattamento dei dati personali nella pubblicazione di atti e delibere nelle aree dei siti istituzionali dedicate alla pubblicazione della normativa e degli atti di regioni ed enti locali, nonché nell'albo pretorio *online*.

Il Garante ha già esaminato la relativa problematica con il provvedimento recante le "Linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul *web*" del 2 marzo 2011 (in G.U. 19 marzo 2011, n. 64 [doc. *web* n. 1793203]) (cfr. Relazione 2010, pag. 54) individuando un primo quadro unitario di misure e accorgimenti destinati a tutte le pubbliche amministrazioni che effettuano, in attuazione alle disposizioni normative vigenti, attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli soggetti.

A titolo esemplificativo, si ricorda l'esperienza di un cittadino che aveva segnalato al Garante la diffusione di dati personali contenuti in una deliberazione di giunta del 2005 e in una determinazione amministrativa del 2004 pubblicate nel sito *web* del Comune di Padova, relative a un contenzioso giudiziario. A seguito dell'intervento del Garante, il comune si è adeguato alle indicazioni contenute nelle linee-guida citate, rendendo non più accessibile la documentazione contenente i dati personali del segnalante (nota 13 giugno 2011).

Analogamente, in relazione alla pubblicazione sul sito *web* del Comune di Bari dei nominativi dei soggetti esclusi dalle graduatorie relative alla concessione del contributo integrativo per il pagamento del canone di locazione, l'Amministrazione ha provveduto a rimuovere il relativo file perché pubblicato in violazione dell'art. 19, comma 3, del Codice che ammette la diffusione di dati personali unicamente quando è prevista da una norma di legge o di regolamento (nota 2 agosto 2011).

In diverso ambito, si segnala, inoltre, il provvedimento con cui è stato dichiarato non conforme alla disciplina sulla protezione dei dati personali il trattamento, effettuato dal Consiglio di presidenza della giustizia tributaria, di dati personali relativi a un partecipante a una procedura concorsuale per posti vacanti di vice-presidente di sezione di talune commissioni tributarie provinciali, in quanto era stata pubblicata in forma integrale, mediante affissione presso gli uffici di segreteria delle Commissioni stesse, la delibera di rettifica del punteggio delle graduatorie relative all'interessato, contenenti anche valutazioni e apprezzamenti sullo stesso, anziché disporre la pubblicazione della sola parte riguardante la rettifica del punteggio (provv. 22 settembre 2011 [doc. *web* n. 1844190]).

Con specifico riferimento alla pubblicazione di atti e delibere contenenti dati personali nell'albo pretorio *online* degli enti locali, l'Autorità ha avviato numerose istruttorie a fronte delle quali, data la specificità della materia, è attualmente in corso l'elaborazione di nuove linee-guida al fine di individuare un quadro unitario di misure e di accorgimenti utili per le amministrazioni interessate nell'attività di gestione e pubblicazione di atti e documenti nell'albo pretorio *online* presente sui siti istituzionali di comuni e province.

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.

Si segnala la richiesta di chiarimenti del Comune di Muros in relazione alla possibilità di rilasciare ad altro comune i dati relativi a minori di età tra 12 e 36 mesi. In merito il Garante, nel ribadire che la comunicazione di dati personali da parte dei soggetti pubblici ad altri soggetti pubblici è ammessa in primo luogo quando è prevista da un atto normativo (art. 19, comma 2, del Codice), ha evidenziato che in ambito anagrafico, la normativa di settore sancisce per l'ufficiale di anagrafe la possibilità di rilasciare legittimamente gli elenchi degli iscritti nell'anagrafe della popolazione residente alle *"amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità"* (art. 34, commi 1 e 2, d.P.R. 30 maggio 1989, n. 223) (nota 26 ottobre 2011).

Sotto altro profilo, il Comune di Vobbia ha chiesto l'intervento del Garante in ordine alla prassi di alcuni comuni di comunicare ai partiti politici i dati contenuti nelle liste anagrafiche della popolazione residente. In proposito, l'Autorità ha rappresentato che con il provvedimento del 7 aprile 2011 (in G.U. 15 aprile 2011, n. 87 [doc. *web* n. 1804225]) è stato precisato che *"partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati possano prescindere dal rendere l'informativa agli interessati, sino al 30 settembre 2011, solo se: 1) i dati siano raccolti direttamente da pubblici registri, elenchi, atti o altri documenti conoscibili da chiunque senza contattare gli interessati, oppure 2) il materiale propagandistico sia di dimensioni ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non renda possibile inserire un'idonea informativa anche sintetica"*. Tale provvedimento

richiama, a sua volta, il vigente "decalogo" del Garante in materia di propaganda elettorale (provv. 7 settembre 2005, in G.U. 12 settembre 2005, n. 212 [doc. *web* n. 1165613]) con il quale sono stati indicati i presupposti e le garanzie in base alle quali partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati possono utilizzare lecitamente dati personali a fini di comunicazione politica, nonché di propaganda elettorale e referendaria. Nello specifico è stato previsto che *"possono essere anzitutto utilizzati, senza il preventivo consenso degli interessati, i dati contenuti nelle liste elettorali che ciascun comune tiene, aggiorna costantemente e rilascia in copia anche su supporto elettronico"* (par. 2, lett. *a*)), mentre non sono utilizzabili, fra l'altro, per propaganda, neanche da parte di titolari di cariche elettive, i dati dell'*"anagrafe della popolazione residente, utilizzabile però per la comunicazione istituzionale di amministrazioni pubbliche"* (par. 3) (nota 13 maggio 2011).

Con il provvedimento citato, a differenza dei precedenti provvedimenti di esonero in materia elettorale, il Garante ha, altresì, precisato che gli abbonati presenti negli elenchi telefonici (i cui dati possono essere trattati per finalità di *marketing* se non sono iscritti nel Registro delle opposizioni) possono essere contattati telefonicamente da partiti politici e candidati per finalità di propaganda elettorale solo previa manifestazione espressa del consenso.

Per altro verso, ancora in materia di consultazioni elettorali, si ricorda, inoltre, il parere favorevole espresso dal Garante, a seguito della richiesta formulata dalla Provincia di Bolzano, sullo schema di disegno di legge provinciale riguardante l'introduzione del voto per corrispondenza nella provincia autonoma (parere 20 ottobre 2011 [doc. *web* n. 1851426]) (v. *infra* par. 3.4).

3.4. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

Le questioni riguardanti il trattamento dei dati personali presso gli enti locali hanno evidenziato problematiche eterogenee.

In merito, si menziona il parere espresso al Ministero dell'interno in ordine ad uno schema di decreto ministeriale recante il nuovo regolamento di gestione dell'Indice nazionale delle anagrafi. Tale parere tiene conto degli approfondimenti e delle indicazioni rese dall'Ufficio del Garante ai competenti uffici del predetto Ministero nel corso di alcune riunioni, relative

alle modalità di esercizio dei diritti di cui all'art. 7 del Codice in relazione ai dati personali contenuti nell'INA; alle misure volte ad assicurare la rettificazione e l'aggiornamento dei dati personali trattati; alle modalità di espletamento e alla disciplina della vigilanza sulla tenuta delle anagrafi; alle disposizioni relative alle misure idonee a garantire la tracciabilità delle attività svolte nell'ambito del sistema informativo in esame (provv. 24 giugno 2011 [doc. *web* n. 1826698]).

Sotto altro profilo, si segnala ancora la richiesta di chiarimenti formulata dal Comune di Arzignano in ordine all'iniziativa dell'amministrazione di offrire a tutti gli assessori e consiglieri la possibilità di sottoporsi, in forma volontaria e consensuale, a un *drug test* per l'accertamento di assunzione di sostanze stupefacenti.

Al riguardo è stato fatto presente che non è compito del Garante valutare se l'iniziativa volta a somministrare *drug test* ad assessori e consiglieri comunali rientri nelle attività istituzionali dell'ente locale e che in ordine alla possibilità di pubblicare "i dati sensibili relativi all'accertamento", si deve aver presente che la disciplina in materia di protezione dei dati personali prevede un espresso divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (art. 22, comma 8, del Codice).

È stato, altresì, fatto presente che, allo stato, la sottoposizione all'accertamento di assenza di tossicodipendenza –prima dell'assunzione in servizio e, successivamente, ad accertamenti periodici– è prevista dalla specifica normativa di settore solo per gli *"appartenenti alle categorie di lavoratori destinati a mansioni che comportano rischi per la sicurezza, la incolumità e la salute dei terzi, individuate con decreto del Ministro del lavoro e della previdenza sociale, di concerto con il Ministro della sanità"* (art. 125, comma 1, d.P.R. 9 ottobre 1990, n. 309) (nota 30 maggio 2011).

Con specifico riguardo al trattamento dei dati effettuato da soggetti esterni all'amministrazione comunale per l'esercizio di funzioni istituzionali (*outsourcing*) è stato segnalato a questa Autorità che un comune si era avvalso, per la redazione dei verbali di infrazione al codice della strada e per la rilevazione fotografica degli illeciti amministrativi, del contributo di una società privata esterna. Dagli atti dell'istruttoria è emerso, altresì, che alcuni dipendenti di tale società erano stati investiti direttamente dal sindaco dell'esercizio delle

funzioni comunali di prevenzione e accertamento delle violazioni in materia di sosta, attraverso la nomina ad ausiliari del traffico (l. 15 maggio 1997, n. 127). In merito il Garante ha rappresentato che nel trattamento di dati personali connesso allo svolgimento dei propri compiti istituzionali, ciascun soggetto pubblico può avvalersi del contributo di soggetti esterni, affidando a essi determinate attività che restano nella sfera della titolarità dell'amministrazione stessa e che non comportano decisioni di fondo sulle finalità e sulle modalità di utilizzazioni dei dati. Tuttavia, in questo caso, è necessario che l'amministrazione –in qualità di titolare del trattamento– designi il soggetto esterno come "responsabile del trattamento" con un apposito atto scritto che specifichi analiticamente i compiti a esso affidati (art. 29 del Codice). In caso contrario, il trattamento di dati personali si configura come una comunicazione esterna e, in quanto tale, è assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice). Analogamente, è stato fatto presente che le persone fisiche che materialmente trattano i dati personali sia del comune sia del soggetto privato esterno devono essere designate "incaricati del trattamento" con un atto scritto che individui puntualmente l'ambito del trattamento che essi possono effettuare (art. 30 del Codice) (nota 30 maggio 2011).

Si segnala infine che il Garante ha espresso parere favorevole sullo schema di disegno di legge provinciale riguardante l'introduzione del voto per corrispondenza nella Provincia autonoma di Bolzano.

Gli elettori, residenti all'estero o dimoranti fuori provincia e interessati a questa modalità di esercizio del diritto di voto, devono farne apposita richiesta al comune nelle cui liste elettorali sono iscritti. Il comune trasmette, poi, all'ufficio elettorale centrale tutta la documentazione necessaria alla formazione della lista dei cittadini che votano per posta. Al termine della procedura, all'elettore viene recapitato un plico contenente l'informativa sul trattamento dei dati personali e la documentazione necessaria per l'espressione del voto.

L'Autorità, limitatamente agli aspetti di sua competenza, ha rilevato che la disciplina dell'esercizio del diritto di voto per corrispondenza individua adeguate misure e accorgimenti a tutela dei dati personali degli elettori. Sulla base, infatti, delle precisazioni fornite dalla provincia in merito all'informativa trasmessa agli elettori, ai tempi e alle finalità di

conservazione della lista formata a cura dell'ufficio elettorale centrale, risulta che i dati personali di chi intende esercitare il voto per corrispondenza saranno trattati esclusivamente per le finalità connesse all'espletamento della consultazione elettorale di riferimento (parere 20 ottobre 2011 [doc. *web* n. 1851426]).

3.5. COMUNICAZIONI DI DATI PERSONALI TRA SOGGETTI PUBBLICI

Nell'anno di riferimento sono pervenute diverse comunicazioni da parte di soggetti pubblici riguardanti la trasmissione ad un altro soggetto pubblico, in assenza di una norma che lo preveda, di dati personali –diversi da quelli sensibili e giudiziari– necessari per lo svolgimento di funzioni istituzionali (artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice).

In proposito, si segnala, fra le altre, la comunicazione effettuata dal Comune di Talana per trasmettere al Consiglio nazionale delle ricerche e Istituto di genetica delle popolazioni di Sassari (Cnr-Igp) i nominativi, gli indirizzi e i numeri di telefono degli emigrati con i quali l'ente ha mantenuto un contatto, per coinvolgere anche questi soggetti nelle ricerche scientifiche sulla salute dei cittadini e la prevenzione di malattie genetiche già effettuate dal Cnr-Igp sulla popolazione di Talana.

Al riguardo, in relazione alle esigenze evidenziate con la suddetta comunicazione, il Garante ha rappresentato di non avere osservazioni da formulare in ordine alla comunicazione all'Istituto di genetica dei dati personali sovraindicati, sempre che i medesimi dati fossero stati legittimamente raccolti e trattati da parte del Comune di Talana per lo svolgimento delle proprie funzioni istituzionali.

L'Autorità, in tale occasione, ha, altresì, precisato che l'iniziativa descritta doveva, comunque, avvenire nel rispetto di opportune garanzie a tutela degli interessati anche attraverso il conferimento di un'idonea informativa circa il trattamento che sarebbe stato svolto dal Cnr-Igp (con particolare riferimento all'origine dei dati), assicurando la volontarietà dell'adesione dei soggetti coinvolti nonché la cancellazione dei dati delle persone non intenzionate a partecipare alla predetta ricerca in conformità alla normativa di settore (cfr. art. 13 del Codice e relativo Allegato A.4. contenente il "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici") (nota 5 dicembre 2011).

Si segnala altresì il caso di una prefettura, la quale a seguito di una segnalazione ricevuta dai Carabinieri, nell'ambito della procedura *ex* art. 121 del d.P.R. n. 309/1990, ha chiesto chiarimenti al Garante in ordine alla possibilità di trasmettere ad un comune, ai sensi degli artt. 19, comma 2, e 39 del Codice, taluni dati personali riguardanti lo stato di tossicodipendenza di un cuoco, suo dipendente addetto ad una mensa scolastica, in considerazione dei rischi per la sicurezza, l'incolumità e la salute dei frequentatori della mensa stessa. Al riguardo, l'Ufficio ha evidenziato che la disciplina sulle comunicazioni inviate al Garante (contenuta nei citati artt. 19 e 39 del Codice), riguarda esclusivamente le comunicazioni tra soggetti pubblici aventi ad oggetto dati non sensibili. Ha, inoltre, precisato che la Conferenza unificata Stato–Regioni, città e autonomie locali, ha stipulato un'intesa in materia di accertamenti di assenza di assunzione di sostanze stupefacenti e psicotrope per i lavoratori impiegati in mansioni che comportano rischi per la sicurezza, l'incolumità e la salute degli stessi e dei terzi (con provvedimento Conferenza unificata del 30 ottobre 2007 - "Intesa, ai sensi dell'art. 8, comma 6, della legge 5 giugno 2003, n. 131, in materia di accertamento di assenza di tossicodipendenza" (Repertorio atti n. 99/CU), pubblicato in G.U. 15 novembre 2007, n. 266) e che la professione di *"cuoco addetto alla mensa scolastica"* non risulta annoverata tra le mansioni a rischio individuate nell'allegato 1 che forma parte integrante dell'intesa stessa (nota 27 aprile 2011).

Enac

Appare per alcuni profili connessa alla precedente, una segnalazione relativa all'Ente nazionale per l'aviazione civile (Enac), che aveva con ordinanza obbligato gli esercenti il servizio di noleggio con conducente (ncc) ad esporre sul parabrezza del veicolo, per i controlli degli organi di vigilanza, il foglio di servizio contenente oltre ai dati identificativi della società di noleggio, i dati anagrafici del passeggero, e l'indicazione della destinazione dello stesso.

Al riguardo l'Ufficio ha avviato un'istruttoria per individuare le specifiche esigenze che rendevano necessario il suddetto trattamento e per accertare che in tale ambito fossero rispettati i princìpi di pertinenza, non eccedenza e proporzionalità dei dati (art. 11 del Codice) invitando altresì l'ente a specificare, in particolare, se le citate informazioni potessero essere riportate nel documento con modalità tali da non consentire la loro diretta visibilità se non in caso di richiesta di esibizione da parte degli organi di vigilanza.

Facendo seguito all'intervento dell'Ufficio, l'Enac ha comunicato di aver provveduto ad integrare l'ordinanza oggetto della segnalazione in modo conforme a quanto previsto dalla normativa sulla protezione dei dati personali, prevedendo, in particolare, che il foglio di servizio di cui devono essere muniti gli esercenti l'attività di noleggio con conducente non in possesso di subconcessione aeroportuale venga *"conservato in modo tale che le informazioni contenute non siano direttamente visibili, ma immediatamente disponibili in caso di richiesta di esibizione da parte degli Organi di vigilanza"* (nota 17 febbraio 2012).

3.6. L'ATTIVITÀ GIUDIZIARIA

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2011 sono pervenute segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 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 dettaglio, in un reclamo l'interessato lamentava la presenza in internet del proprio nominativo nella prima pagina della perizia, prodotta all'Ufficio, allegata ad un avviso d'asta.

In un caso analogo, veniva segnalata in particolare la pubblicazione sul sito internet di una società di aste immobiliari di una perizia allegata all'avviso d'asta, anch'essa prodotta, che recava, tra le altre informazioni, anche il nome e i dati anagrafici dell'interessata.

Le verifiche effettuate nei due casi dall'Autorità sui siti in questione hanno permesso di rilevare la presenza delle procedure oggetto di segnalazione, prive però dei dati personali dei segnalanti e degli altri debitori, evidentemente già rimossi in seguito alle lamentele degli interessati.

L'Autorità ha comunque sollecitato l'attenzione della società di aste *online* e dei presidenti dei tribunali interessati, anche richiamando il provvedimento del 7 febbraio 2008 ([doc. *web* n. 1490838], v. Relazione 2007, p. 55) con il quale il Garante ha evidenziato, in particolare, 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, al fine di evitare il ripetersi di analoghi episodi (note 4 aprile e 15 novembre 2011).

In ulteriori due segnalazioni, veniva lamentato, in un caso, l'invio a numerosi cittadini residenti nel comune dell'interessato di un volantino contenente informazioni volte a reperire l'immobile di sua proprietà oggetto di vendita con incanto, nell'altro, la pubblicazione della precisa denominazione con cui l'immobile oggetto della procedura era conosciuto nella zona ove era situato. L'Autorità ha chiarito che nelle due fattispecie non vi era stata alcuna violazione della normativa in materia di protezione dei dati personali, in quanto le due pubblicazioni non contenevano dati personali dei debitori o di soggetti estranei alla procedura, bensì solo informazioni che permettevano di individuare con univocità gli immobili oggetto di espropriazione (note 4 gennaio e 25 maggio 2011).

Procedure concorsuali

Un sindacato ed alcuni cittadini avevano lamentato che collegandosi al sito internet "Portale delle procedure concorsuali", gestito dal Ministero della giustizia, con le credenziali fornite ai creditori interessati ad una procedura esecutiva, ogni creditore poteva accedere non solo alla propria scheda personale, bensì all'intero "Progetto di stato passivo" della procedura, ottenendo in tal modo informazioni dettagliate in relazione a qualsivoglia posizione di credito nei confronti del debitore; inoltre i nomi dei creditori non risultavano oscurati.

All'esito dell'istruttoria, sentito anche il Ministero della giustizia, il Garante ha ritenuto corretto il trattamento dei dati in oggetto.

In particolare, per quanto attiene alle norme specifiche relative alle procedure concorsuali, l'Autorità ha rilevato che il r.d. 16 marzo 1942, n. 267 (cd. "legge fallimentare") stabilisce l'obbligo per gli organi della procedura di mettere a disposizione dei creditori il progetto di stato passivo e lo stato passivo nella loro interezza, ossia in forma integrale. Né l'indicazione del nominativo dei creditori inseriti in tali atti può ritenersi eccedente, ai sensi dell'art. 11 del Codice, rispetto agli scopi che la normativa concorsuale si prefigge, in quanto l'esatta identificazione dei creditori insinuati nella procedura è necessaria per la tutela dei diritti, eventualmente confliggenti, vantati dai vari creditori (si pensi, ad esempio, all'accertamento della *scientia decoctionis* in capo ad un creditore, al fine di ottenere una revocatoria, oppure alla contestazione di un privilegio) (nota 20 luglio 2011).

Assenze per malattia dei giudici tributari

È pervenuta una segnalazione di alcuni giudici di una Commissione tributaria regionale relativa alla risoluzione con cui il Consiglio di presidenza della giustizia tributaria aveva indicato la documentazione medica, dettagliata, da presentare al Consiglio stesso da parte dei giudici in caso di assenze per malattia e che, in caso di patologie di particolare gravità, doveva comprendere anche la diagnosi.

Acquisite informazioni preliminari, l'Autorità ha avviato un procedimento amministrativo nei confronti del Consiglio di presidenza, ritenendo che la richiesta di indicare la diagnosi violasse i princìpi di pertinenza e di non eccedenza nel trattamento dei dati personali rispetto alle finalità per cui le informazioni vengono raccolte (art. 11, comma 1, lett. *d*) del Codice) e di indispensabilità del trattamento dei dati sensibili da parte dei soggetti pubblici (art. 22 del Codice), richiamati anche nel punto 8.2. delle "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (deliberazione 14 giugno 2007 [doc. *web* n. 1417809]).

Successivamente il Consiglio di presidenza ha informato il Garante di avere modificato la suddetta risoluzione, che ora non contiene più la richiesta che i certificati medici dei giudici tributari siano dettagliati, né che sia riportata la diagnosi in caso di certificati relativi a patologie di particolare gravità.

Il Garante ha ritenuto tale regolamentazione conforme alla normativa in materia di protezione dei dati personali (nota 29 settembre 2011).

Accesso ai dati relativi a procedimenti giudiziari

Sono giunti all'Autorità due quesiti, posti il primo dal presidente di un tribunale, il secondo da una sezione giurisdizionale regionale della Corte dei conti, concernenti il regime di pubblicità dei dati attinenti a procedimenti giudiziari.

Nel primo caso, una testata giornalistica televisiva aveva chiesto di consultare gli atti di un procedimento penale, ivi compreso il materiale fotografico e videoregistrato allegato agli atti, che intendeva utilizzare per la realizzazione di un programma avente ad oggetto vicende giudiziarie.

Nel secondo, un avvocato aveva chiesto di accedere ai ruoli delle udienze della sezione.

In entrambe le fattispecie l'Autorità ha ricordato che la visione e il rilascio di estratti e di copie di atti giudiziari, la conoscenza dell'esito e del calendario dei processi, la pubblicità

delle udienze e la consultazione dei registri relativi ai procedimenti giudiziari rimangono assoggettati alle pertinenti disposizioni processuali (art. 51 del Codice).

Poiché si tratta di attività svolte *"per ragioni di giustizia"* (art. 47, comma 2, del Codice), la decisione sull'accesso ai dati deve essere ricavata dall'autorità giudiziaria nel quadro delle norme processuali, tenendo conto delle specifiche finalità perseguite dal soggetto richiedente.

L'Autorità ha, peraltro, ribadito che restano fermi, in quanto applicabili anche a tali attività, i princìpi posti dall'art. 11 del Codice, in base ai quali l'accesso ai dati personali può essere consentito solo previa verifica dell'esistenza di uno scopo determinato, esplicito e legittimo (comma 1, lett. *b*)) e relativamente alle sole informazioni pertinenti e non eccedenti rispetto allo scopo medesimo (comma 1, lett. *d*)), sollecitando quindi le autorità giudiziarie a valutare attentamente la possibilità di omettere informazioni atte a consentire l'identificazione dei soggetti coinvolti nei giudizi, ove ciò non sia strettamente necessario al perseguimento delle finalità perseguite dai richiedenti (note 5 e 21 gennaio 2011).

Pubblicazione di atti processuali

Il destinatario di un'ordinanza di custodia cautelare in carcere, diffusa su siti internet a corredo di una notizia concernente un presunto caso di corruzione, si è rivolto al Garante lamentando un'illecita diffusione di dati riservati, quali numeri delle utenze cellulari, indirizzi dei luoghi di residenza e domicilio e targhe di autovetture.

All'esito dell'istruttoria, rilevato che la pubblicazione del provvedimento integrava un trattamento a cui doveva essere applicata la normativa *privacy* in materia di attività giornalistica, il Garante, pur riconoscendo il diritto alla manifestazione del pensiero da parte dell'associazione che gestiva i siti, ha ritenuto che la diffusione dei numeri di telefono, degli indirizzi e dei numeri di targa di autovetture del segnalante e di altre persone citate nell'ordinanza abbia violato il principio di essenzialità dell'informazione, trattandosi di dati personali sicuramente sovrabbondanti e non indispensabili per rappresentare la vicenda giudiziaria.

Il Garante ha quindi vietato l'ulteriore diffusione dei dati, disponendo la cancellazione delle informazioni eccedenti dai due siti (provv. 5 maggio 2011 [doc. *web* n. 1827129]).

3.6.1. L'informatica giuridica

Linee-guida per la diffusione dei provvedimenti giudiziari

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

Con riferimento a questa ipotesi, sono pervenuti all'attenzione dell'Autorità casi di cittadini che non avevano chiesto l'anonimizzazione della sentenza nel corso del giudizio.

In un caso, una interessata aveva lamentato la reperibilità in internet di una sentenza del Consiglio di Stato che rendeva noti particolari relativi alla propria vita sessuale.

In un altro caso, è pervenuto un reclamo nel quale l'interessato aveva lamentato la agevole reperibilità nei motori di ricerca presenti in rete di una sentenza di un tribunale amministrativo regionale che riportava informazioni relative a provvedimenti di natura penale che lo riguardavano e che gli causavano estremo disagio nell'ambito della propria vita personale e professionale.

Nei due casi il Garante ha sottoposto le vicende all'attenzione dei rispettivi organi di giustizia amministrativa, per l'eventuale anonimizzazione d'ufficio delle sentenze, anche secondo quanto suggerito nelle menzionate linee-guida, oppure, in alternativa, per l'adozione di accorgimenti tecnici idonei ad evitare l'indicizzazione nei motori di ricerca delle pronunce pubblicate sui rispettivi siti istituzionali (note 25 febbraio e 18 novembre 2011).

In entrambi i casi i giudici amministrativi hanno disposto l'oscuramento dei dati personali presenti nei rispettivi provvedimenti.

Sono giunti all'Autorità due quesiti relativi alla diffusione di provvedimenti giurisdizionali per finalità di informazione giuridica.

Con il primo, il Ministero della giustizia aveva chiesto se poteva procedere alla pubblicazione sul suo sito in forma integrale, con i dati identificativi dei soggetti citati nelle sentenze, delle pronunce della Corte europea dei diritti dell'uomo.

Nel fornire riscontro, l'Autorità ha confermato, in primo luogo, che alla Corte non può applicarsi la normativa italiana posta nella materia dagli artt. 51 e 52 del Codice e dalle linee-guida del Garante in tema di anonimizzazione delle sentenze avanti alla autorità giudiziaria, ma che la stessa si applica nei confronti di chiunque diffonda provvedimenti giurisdizionali per l'indicata finalità, unitamente ad ogni altra disposizione recante specifici divieti di pubblicazione dei dati di individuate categorie di interessati (quali minori, parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone, persone offese da atti violenza sessuale). L'Autorità ha, altresì, sottolineato la particolare responsabilità nell'attenta valutazione dell'opportunità di procedere all'anonimizzazione che incombe sui soggetti che diffondono tali provvedimenti tanto più nei casi, come quello oggetto del quesito, in cui la diffusione delle sentenze non è preceduta dalla preventiva procedura di garanzia volta alla tutela dell'identità delle persone citate nelle pronunce (nota 9 novembre 2011).

Con il secondo quesito un consiglio dell'ordine degli avvocati aveva chiesto se poteva costituire violazione della normativa di protezione dei dati la diffusione da parte del consiglio ai propri iscritti, per finalità di informazione giuridica, di sentenze emesse dalla locale magistratura.

Anche in questo caso l'Autorità, nel sottolineare che il Codice e le linee-guida del Garante favoriscono la più ampia diffusione dei provvedimenti giurisdizionali, e che, quindi, non si pongono, in linea generale, impedimenti alla realizzazione del progetto, ha ricordato la necessità di rispettare le disposizioni ed i divieti di pubblicazione vigenti a tutela di particolari categorie di interessati (nota 6 dicembre 2011).

3.6.2. Notificazioni di atti e comunicazioni

Nel 2011 va registrato con soddisfazione l'azzeramento quasi totale delle segnalazioni circa le modalità di notificazione di atti giudiziari in modo non conforme alle prescrizioni del Codice. Al riguardo merita una citazione in questa sede una segnalazione con la quale veniva lamentata la notificazione di un atto citazione in un giudizio penale, effettuata lasciando un plico non sigillato presso il portiere del condominio di residenza dell'interessato, in sua assenza.

Il Garante, al riguardo, ha rappresentato che, com'è noto, a decorrere dal 1° gennaio 2004 l'art. 174 del Codice ha introdotto particolari modalità di notifica, ove questa non possa essere eseguita nelle mani proprie del destinatario (inserimento di copia dell'atto in busta chiusa e sigillata su cui viene apposto il solo numero cronologico della notificazione; annotazione nella relazione in calce all'originale e alla copia dell'atto stesso). Questo per impedire a terzi di venire a conoscenza del contenuto dell'atto, di regola contenente dati personali particolarmente delicati.

L'Autorità ha richiamato l'attenzione dell'Ufficio notificazioni e protesti coinvolto nel rispetto di tali norme, al fine della tutela della riservatezza dei destinatari degli atti (nota 6 ottobre 2011). Detto Ufficio ha rappresentato che l'ufficiale giudiziario incaricato della notifica ha presentato le proprie giustificazioni adducendo un disguido involontario e provvedendo ad una nuova notifica secondo i criteri previsti dall'art. 174 del Codice.

Analogamente l'Ufficio, con riferimento ad una notificazione di un avviso di pagamento relativo alla Tarsu effettuata da parte di un comune, ha ricordato che sulla busta da notificare devono essere leggibili solo le informazioni necessarie all'invio della comunicazione al destinatario e non ulteriori dati eccedenti come il codice fiscale della destinataria dell'avviso (artt. 11, comma 1 e 174 del Codice) (nota 2 febbraio 2012).

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

Provvedimenti in materia di protesi mammarie

Alla fine del 2011, il Garante è stato interpellato dal Ministro della salute su uno schema di ordinanza di necessità e urgenza, relativa all'adozione di provvedimenti in materia di protesi mammarie (*Poly Implants Prothese*, cosiddette PIP), da emanarsi ai sensi dell'art. 32, comma 1, l. 23 dicembre 1978, n. 833 (parere 29 dicembre 2011 [doc. *web* n. 1863619]. Lo schema di provvedimento ha tenuto conto delle indicazioni fornite dall'Ufficio nel corso di contatti informali con il Ministero, volti a rendere sotto ogni profilo effettivo il diritto alla protezione dei dati personali delle persone interessate, ed è stato pertanto valutato favorevolmente dal Garante. Esso prevede l'obbligo per le strutture ospedaliere e ambulatoriali di redigere un elenco nominativo delle pazienti sottopostesi a interventi di applicazione di PIP che dovrà rimanere nella loro esclusiva disponibilità a fini assistenziali e di sorveglianza sanitaria. È sancito inoltre l'obbligo, in capo alle strutture sanitarie, di notificare alla competente azienda unità sanitaria locale o direttamente alla competente autorità regionale, mediante un modulo reso disponibile sul sito istituzionale del Ministero, le informazioni relative alla data dell'intervento di mammoplastica effettuato. I dati, così raccolti, dovranno poi essere comunicati, via PEC, al Ministero, *"garantendo la tutela dell'anonimato dei dati rilevati e comunque nel rispetto"* di quanto previsto dal Codice, sempre avvalendosi di una scheda resa disponibile sul sito istituzionale dello stesso Ministero.

Pagamento del ticket: procedure per l'accertamento del reddito degli assistiti presso le farmacie

Specifiche indicazioni sono state rese dall'Ufficio del Garante ai competenti uffici dei Ministeri dell'economia e della finanze e della salute, nonché di alcune regioni, in relazione ai trattamenti di dati effettuati dalle farmacie per verificare il diritto dell'assistito al pagamento del ticket in relazione alla fascia di reddito.

Al riguardo, erano pervenute all'Autorità numerose segnalazioni con le quali si lamentava che alcune regioni, ai fini dell'applicazione del ticket, richiedevano agli utenti del servizio sanitario nazionale di autocertificare al farmacista la fascia di reddito di appartenenza, con modalità tali da non garantire un'adeguata protezione dei dati personali dei pazienti. Alcune

regioni, infatti, in attuazione di quanto disposto dalla manovra economica 2011, ovvero il rispristino della quota fissa di compartecipazione alla spesa sanitaria (art. 17, d.l. 6 luglio 2011, n. 98, convertito, con modificazioni, dalla l. 15 luglio 2011, n.111), hanno deciso di adottare modalità alternative di compartecipazione, differenziando il ticket in base alla fascia di reddito familiare. Tuttavia, le modalità previste non garantivano la riservatezza degli interessati i quali, per usufruire delle esenzioni sul ticket, erano costretti a comunicare la loro condizione reddituale al farmacista, magari in presenza di altri clienti, o alle persone che eventualmente acquistavano medicinali per loro conto.

Sul tema, il Ministero dell'economia e delle finanze ha predisposto uno schema di linee di indirizzo in materia di misure regionali di compartecipazione alla spesa sanitaria per fasce di reddito, il quale, recependo le indicazioni fornite dall'Ufficio volte a garantire sul territorio regionale uno *standard* omogeneo della riservatezza degli assistiti, è stato valutato favorevolmente dal Garante parere 26 ottobre 2011 [doc. *web* n. 1851679]. In conformità con quanto previsto a livello nazionale (cfr. d.m. 11 dicembre 2009, sul cui schema il Garante ha reso parere favorevole in data 8 aprile 2009 [doc. *web* n. 1611955]), le nuove misure prospettate dal Ministero prevedono che sia il medico stesso ad apporre sulla ricetta un codice teso a identificare, non in chiaro, la fascia di reddito dell'assistito. All'atto della prescrizione, il medico dovrà verificare il menzionato codice collegandosi al sistema informatico "tessera sanitaria" oppure utilizzando l'apposita documentazione cartacea o digitale predisposta dalla azienda sanitaria locale (alla stregua di quanto previsto dall'art. 50, l. 24 novembre 2003, n. 326 e dal d.P.C.m. 26 marzo 2008).

4.1.2. I trattamenti per fini amministrativi

Schema-tipo di regolamento per trattamenti di dati sensibili e giudiziari da parte di regioni e Asl

Nel 2011 sono proseguite le attività del tavolo di lavoro interregionale istituito sulla revisione dello schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e di altri enti, tra cui le aziende sanitarie locali (v. parere favorevole del Garante 13 aprile 2006 [doc. *web* n. 1272225]). Ai lavori, conclusi a fine anno, l'Ufficio ha partecipato attivamente, condividendo l'esigenza, manifestata da parte di più enti, di aggiornare lo schema-tipo, anche alla luce delle numerose modifiche normative sopravvenute.

Una volta approvato dalla Conferenza delle regioni e delle province autonome e sottoposto all'esame Autorità per il necessario parere, il testo aggiornato dello schema-tipo consentirà a tali enti di disporre di uno quadro aggiornato di garanzie in conformità al quale potranno essere adottati i necessari atti regolamentari.

Sistema informativo per il monitoraggio dell'assistenza erogata presso gli *hospice*

In data 11 ottobre 2011, il Garante ha inoltre dato parere favorevole senza osservazioni [doc. *web* n. 1851388] allo schema di decreto del Ministero della salute che istituisce il sistema informativo per il monitoraggio dell'assistenza erogata presso gli *hospice*, le strutture sanitarie residenziali per malati terminali idonee a garantire l'accesso alle cure palliative e alla terapia del dolore (cfr. artt. 5 e 9, l. 15 marzo 2010, n. 38). Lo schema aveva infatti già recepito le indicazioni fornite dall'Ufficio del Garante al Ministero nel corso di riunioni e contatti informali quali i presupposti della rilevazione e la precisazione delle finalità del monitoraggio attivato presso il Ministero della salute, indicate dalla l. n. 38/2010; i parametri ai quali devono conformarsi le trasmissioni telematiche dei dati al sistema; l'autenticazione dei soggetti abilitati all'accesso; il rispetto del principio di proporzionalità nel trattamento dei dati, con particolare riguardo alle informazioni relative alle patologie da cui è affetto l'interessato; l'esigenza di utilizzare tecniche di cifratura al fine di rendere i suddetti dati temporaneamente inintelligibili anche a chi è autorizzato ad accedervi.

Il sistema, realizzato e gestito dal Ministero della salute, nell'ambito del Nuovo sistema informativo sanitario (Nsis), è costituito da una banca dati alimentata con informazioni, prive di elementi identificativi diretti dei pazienti, fornite dalle regioni e dalle province autonome che, attraverso gli *hospice* presenti nel proprio territorio, abbiano prestato assistenza sanitaria o socio-sanitaria ai cittadini (ivi residenti o meno). Lo schema di decreto prevede infatti che nel sistema, cui affluiscono informazioni, anche di carattere sanitario (caratteristiche dell'assistito, prestazioni erogate, dati sulla presa in carico e conclusione della degenza) non siano presenti i nominativi dei pazienti, i quali dovranno quindi essere sostituiti da un codice univoco, ovvero, ove le regioni e le province autonome non dispongano di adeguati sistemi di codifica, inviati in forma anonima, in conformità a quanto previsto dalla scheda 12 dello schema di regolamento per il trattamento dei dati sensibili e giudiziari effettuato dai predetti enti.

Per garantire la riservatezza dei pazienti, inoltre, il Ministero, le regioni e le province autonome, ai fini del monitoraggio dell'assistenza in materia di cure palliative, terapia del dolore e della spesa sanitaria, potranno accedere soltanto a dati aggregati e mediante chiavi di ricerca che non consentono di consultare dati riferibili a singoli individui. I dati sanitari infine dovranno essere trattati con tecniche crittografiche e archiviati previa separazione dalle altre informazioni. Le medesime tecniche saranno utilizzate al fine di rendere i dati relativi alla patologia da cui è affetto l'interessato temporaneamente inintelligibili anche a chi è autorizzato ad accedervi. Per quanto riguarda la trasmissione dei dati, lo schema di decreto prevede l'adozione di protocolli sicuri e l'autenticazione bilaterale tra i sistemi, basata su certificati digitali emessi da una autorità di certificazione ufficiale.

Linee-guida sulle indagini di *customer satisfaction* in ambito sanitario

I trattamenti di dati effettuati dagli organismi sanitari nell'ambito di iniziative volte a verificare la qualità delle prestazioni rese hanno formato oggetto di apposite linee-guida adottate dal Garante ("Linee-guida in tema di trattamento di dati per lo svolgimento di indagini di *customer satisfaction* in ambito sanitario" del 5 maggio 2011 [doc. *web* n. 1812910]). L'acquisizione delle informazioni al riguardo rilevanti può comportare infatti il trattamento dei dati personali, anche attinenti alla salute, dei cittadini e degli utenti dei servizi prestati, in relazione allo specifico contesto sanitario in cui il sondaggio viene realizzato e a seconda delle modalità di selezione del campione prescelte o di somministrazione del questionario, nonché della tipologia delle informazioni richieste (desumibili ad es. dal tipo di reparto che ha erogato il servizio, dalla prestazione fruita o persino dalla fornitura di particolari ausili).

L'Autorità ha pertanto ritenuto opportuno individuare un quadro unitario di misure e accorgimenti al quale dovranno attenersi gli organismi sanitari pubblici e privati che svolgono indagini sulla qualità dei servizi sanitari offerti.

I sondaggi, indipendentemente dalle modalità prescelte per l'effettuazione (per telefono, per posta, per e-mail, tramite questionari cartacei o form disponibili sul sito istituzionale della struttura sanitaria) possono riguardare esclusivamente informazioni sulla qualità del servizio (accoglienza, tempi di attesa, informazioni ricevute, comfort della struttura), senza entrare nella valutazione degli aspetti sanitari delle prestazioni e delle cure erogate.

Prima di iniziare il sondaggio gli organismi sanitari devono valutare, nel rispetto del principio di necessità, se sia realmente necessario raccogliere dati personali per raggiungere gli scopi del sondaggio, oppure se non sia invece possibile raggiungere i medesimi obiettivi utilizzando informazioni anonime. In questo secondo caso, il trattamento dei dati raccolti non ricade nell'applicazione della normativa in materia di protezione dei dati personali e, di conseguenza, delle linee-guida.

Qualora invece si ritenga necessario acquisire dati personali, la raccolta deve essere effettuata sulla base di idonei presupposti giuridici a seconda che tale attività sia svolta o meno nell'ambito dei compiti del Servizio sanitario nazionale o degli altri organismi sanitari pubblici.

In questo caso, gli organismi privati che svolgono direttamente un'indagine di gradimento sui servizi sanitari, oltre a rispettare le prescrizioni contenute nelle autorizzazioni generali del Garante nn. 2 e 5, devono chiedere il consenso scritto degli utenti coinvolti (art. 26, comma 1, del Codice). Consenso che non deve essere invece richiesto dagli organismi pubblici, anche quando conducono sondaggi attraverso le strutture convenzionate (artt. 18, 20 e 85 del Codice; art. 11, comma 1, d.lgs. n. 286/1999 e artt. 10 e 14 d.lgs. n. 502/1992).

Per la realizzazione di iniziative di *customer satisfaction*, non è invece consentito l'utilizzo di dati sulla vita sessuale degli interessati e le informazioni raccolte non possono essere utilizzate per profilare gli utenti o inviare materiale pubblicitario.

In ogni caso, la partecipazione degli assistiti deve essere sempre su base volontaria.

Le successive fasi di elaborazione e di memorizzazione dei dati raccolti non devono permettere di identificare gli interessati, neanche indirettamente; eventuali dati identificativi vanno quindi distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la registrazione. La comunicazione o la diffusione dei risultati dei sondaggi deve avvenire inoltre sempre in forma anonima o aggregata.

Agli utenti, infine, deve essere assicurata, dagli operatori sia privati sia pubblici, una dettagliata informativa in cui risultino chiari tutti gli aspetti e le modalità del sondaggio. Al fine di agevolare l'indicazione degli elementi essenziali dell'informativa, l'Autorità ha predisposto un modello semplificato allegato alle linee-guida (Allegato 1) che potrà essere

utilizzato dagli organismi sanitari, adattandolo alle modalità prescelte di svolgimento delle indagini, in armonia con i princìpi di semplificazione, armonizzazione ed efficacia previsti dal Codice (art. 2).

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

Anche nel 2011, l'Autorità ha richiamato l'attenzione dei titolari del trattamento operanti in ambito sanitario sulla necessità di garantire il rispetto della dignità della persona e il massimo livello di tutela degli interessati nell'organizzazione delle prestazioni e dei servizi sanitari in conformità alle disposizioni dell'art. 83 del Codice (provv. 9 novembre 2005 [doc. *web* n. 1191411]).

In particolare, il Garante ha precisato che la consegna di certificati medici e di altri documenti che contengono informazioni sulla salute dei pazienti deve avvenire in busta chiusa non solo quando questa viene effettuata nei confronti di soggetti delegati dall'interessato (punto 4, provv. cit.), ma anche nel caso in cui la documentazione sanitaria è consegnata allo stesso interessato da parte di personale non sanitario (personale amministrativo o addetto ad attività di sportello). Queste modalità di consegna dei referti sono state oggetto di specifiche prescrizioni nei riguardi di una Asl –che aveva attivato dei centri prelievi organizzati presso alcuni comuni del territorio all'uopo convenzionati– grazie ad una segnalazione in cui si lamentava che i risultati delle analisi venivano consegnati in cartelline pinzate soltanto sul lato sinistro e, quindi, aperte, potendo essere facilmente letti dagli incaricati del comune addetti al servizio di consegna.

Nel provvedimento con il quale ha dichiarato illecito il trattamento dei dati sanitari così effettuato, il Garante ha sottolineato che il consenso alla comunicazione dei dati sanitari è valido solo se espresso liberamente e per un trattamento chiaramente individuato. Nel caso di specie, invece, non essendo previste modalità alternative di consegna della certificazione rispetto a quella in busta aperta, il consenso risultava necessitato quale conseguenza della scelta di utilizzare i centri prelievo organizzati dal comune. L'Autorità ha inoltre ribadito che sia l'art. 84 del Codice, sia il provvedimento generale del 2005 in materia di tutela della dignità nelle strutture sanitarie (punto 4), prevedono che i dati idonei a rivelare lo stato di

salute possono essere resi noti direttamente all'interessato soltanto da personale medico o da altri professionisti sanitari espressamente incaricati, a condizione che l'atto di incarico individui appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento dei dati (art. 84, comma 2, del Codice).

L'Azienda sanitaria ha poi prontamente adempiuto alle prescrizioni del Garante adottando quale modalità di comunicazione dei dati sanitari agli interessati che si rivolgono ai centri prelievo organizzati presso i comuni, la consegna della relativa certificazione sanitaria in busta chiusa (provv. 24 febbraio 2011 [doc. *web* n. 1797075]).

4.1.4. La ricerca scientifica

Nel corso dell'anno sono considerevolmente aumentate le richieste di autorizzazione aventi ad oggetto trattamenti di dati relativi allo stato di salute effettuati, anche in mancanza del consenso degli interessati, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in ragione della impossibilità di rendere l'informativa ad una parte significativa dei pazienti coinvolti, giustificata da particolari ragioni (cfr. art. 110 del Codice).

Le autorizzazioni sono state accordate in ragione della rilevanza degli scopi scientifici perseguiti, nonché delle difficoltà, rappresentate nei diversi casi, di informare i pazienti per acquisire il loro consenso, trattandosi di studi retrospettivi relativi a cospicui campioni di interessati o effettuati con dati riguardanti individui irrintracciabili, oppure presumibilmente deceduti, considerato anche il periodo di tempo trascorso dal momento in cui i dati a loro riferiti erano stati originariamente raccolti, l'età degli interessati e l'incidenza della mortalità in pazienti affetti dalla patologia oggetto dello studio.

In tutti i casi è stato autorizzato il trattamento delle sole informazioni indispensabili per lo svolgimento degli studi e sono state individuate diverse precauzioni a tutela della riservatezza dei pazienti coinvolti. Queste cautele hanno riguardato diversi profili relativi al trattamento dei dati effettuato per l'esecuzione dello studio, quali le misure opportune per ridurre il rischio di re-identificazione degli interessati (ad es. l'adozione di codici identificativi non direttamente riconducibili ai dati identificativi degli interessati, provv. 15 settembre 2011 [doc. *web* n. 1849964] e provv. 11 ottobre 2011 [doc. *web* n. 1849933] o di misure idonee ad

impedire ai ricercatori di accedere alla lista di de-codifica detenuta dai medici curanti degli interessati, provv. 25 gennaio 2012 [doc. *web* n. 1872084]); la correttezza e la completezza delle indicazioni riportate nel modello di informativa e di raccolta del consenso da sottoporre ai pazienti risultati ancora in vita e reperibili (provv. 15 settembre 2011 [doc. *web* n. 1849964], provv. 11 ottobre 2011 [doc. *web* n. 1849933] e provv. 20 gennaio 2012 [doc. *web* n. 1872049]); nonché gli accorgimenti idonei ad incrementare il livello di sicurezza del trattamento dei dati (v. tra gli altri provv. 21 luglio 2011 [doc. *web* n. 1836317], provv. 22 settembre 2011 [doc. *web* n. 1849897], provv. 11 ottobre 2011 [doc. *web* n. 1849933], provv. 1° dicembre 2011 [doc. *web* n. 1872054] e provv. 25 gennaio 2012 [doc. *web* n. 1872084]) anche in conformità alle "Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" (provv. 24 luglio 2008 [doc. *web* n. 1533155]).

In tale quadro, alla luce dell'esperienza maturata, e al fine di garantire il rispetto dei princìpi di semplificazione anche nello svolgimento degli adempimenti degli obblighi da parte dei titolari del trattamento, l'Autorità ha ritenuto opportuno rilasciare un'autorizzazione generale temporanea, che ha tenuto conto delle più ricorrenti ragioni che hanno reso impossibile fornire l'informativa all'interessato, nella quale sono stati considerati, in particolare, i "motivi etici", riconducibili alla circostanza che i pazienti che si intende coinvolgere nella ricerca ignorino la propria condizione ovvero di "motivi di impossibilità organizzativa", riconducibili alla circostanza che risulti impossibile contattare tali soggetti.

Pertanto non è più necessaria la richiesta, caso per caso, di specifiche autorizzazioni da parte dei titolari del trattamento che, in presenza dei menzionati presupposti, intendano trattare i dati personali dei pazienti in assenza del loro consenso per iniziative di ricerca scientifica in campo medico, biomedico o epidemiologico purché siano rispettate le garanzie e le prescrizioni individuate nella stessa autorizzazione. Prima dell'adozione definitiva, lo schema di autorizzazione è stato preliminarmente sottoposto ad una consultazione pubblica (deliberazione n. 486 del 15 dicembre 2011, in G.U. 3 gennaio 2012, n. 2 [doc. *web* n. 1859602]) per acquisire osservazioni e commenti da parte dei soggetti interessati.

L'autorizzazione, adottata in via definitiva il 1° marzo 2012 (in corso di pubblicazione in G.U. [doc. *web* n. 1878276]) consente di effettuare studi basati su dati idonei a rivelare lo

stato di salute raccolti in precedenza a fini di cura o in altri progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per le stesse finalità a condizione che sul progetto di ricerca sia espresso favorevolmente, con parere motivato, il competente comitato etico a livello territoriale.

I titolari del trattamento che effettuano gli studi in questione dovranno inoltre adottare misure specifiche per non rendere i dati trattati direttamente riconducibili ai pazienti interessati (ad es. adozione di tecniche crittografiche, uso di codici identificativi) e dovranno informare comunque e acquisire il consenso al trattamento dei dati dei pazienti che risultino invece reperibili. Un elevato livello di sicurezza dei dati dovrà essere assicurato in ogni fase della ricerca, adottando opportuni accorgimenti che garantiscano da rischi di accesso abusivo, furto o smarrimento dei supporti di memorizzazione o dei sistemi di elaborazione (ad es. applicando tecnologie crittografiche o misure di protezione che li rendano inintelligibili a personale non autorizzato). Analoghe cautele dovranno essere utilizzate nella trasmissione elettronica dei dati dello studio al promotore della ricerca o al *database* centralizzato in cui sono memorizzati e archiviati. Obbligatorie, infine, le procedure di autenticazione per l'accesso ai dati mediante credenziali di validità limitata alla durata dello studio, procedure per la verifica periodica delle credenziali di autenticazione e sistemi di audit log per il controllo degli accessi e per il rilevamento di eventuali anomalie.

5. I DATI GENETICI

Si è riferito nella Relazione 2010 (cfr. pag. 90), in merito alle procedure avviate per l'aggiornamento dell'autorizzazione generale al trattamento di dati genetici, sentito il Ministero della salute che acquisisce, a tal fine, il parere del Consiglio superiore di sanità (art. 90 del Codice).

Nel parere, il Consiglio superiore di sanità aveva formulato alcuni suggerimenti, tra i quali, quelli riguardanti la definizione di "dato genetico", volti a restringere –rispetto all'autorizzazione allora vigente– la categoria delle informazioni genetiche. Al riguardo l'Ufficio del Garante, all'esito di un doveroso approfondimento –anche alla luce dell'esperienza in ambito comunitario–, aveva modificato la formulazione proposta e aveva richiesto, tramite il Ministero della salute, un nuovo parere del Consiglio superiore di sanità.

Quest'ultimo, con il parere adottato nella seduta del 19 gennaio 2011, si è espresso in senso favorevole a tale definizione di "dato genetico", proposta dal Garante al fine di evitare l'esclusione dal novero dei dati genetici delle informazioni relative alle caratteristiche genotipiche di un individuo le quali, pur non essendo il risultato di analisi genetiche, presentano alcune caratteristiche comuni ai dati genetici, tali da rendere opportuna la previsione di particolari cautele nel loro trattamento.

Su tali basi il Garante, in data 24 giugno 2011, ha approvato in via definitiva il nuovo schema di autorizzazione generale al trattamento dei dati genetici (in G.U. 11 luglio 2011, n. 159 [doc. *web* n. 1822650]). La nuova autorizzazione tiene conto dell'esperienza maturata e delle osservazioni formulate da qualificati esperti della materia, con particolare riferimento, oltre all'aggiornamento delle definizioni utilizzate, anche 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'autorizzazione, inoltre, già rivolta a medici, laboratori di genetica, organismi sanitari, istituti di ricerca, farmacisti, è stata estesa anche gli organismi di mediazione pubblici e privati, introdotti da recente normativa. Tali organismi in caso di trattamento di dati genetici (ad es. procedimenti inerenti il risarcimento del danno derivante da responsabilità medica) dovranno quindi rispettare le prescrizioni ivi contenute.

6. L'ATTIVITÀ DI POLIZIA

6.1. IL CONTROLLO SUL CED DEL DIPARTIMENTO DELLA PUBBLICA SICUREZZA

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

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

In una segnalazione l'interessato aveva lamentato che un Comando dell'Arma dei Carabinieri nel redigere un verbale di accertamento ai sensi dell'art. 5 della l. 689/1981, ne aveva consegnato copia anche all'altro trasgressore, senza omettere le generalità dell'interessato.

Acquisite informazioni dal Comando, l'Autorità ha ritenuto corretto il trattamento dei dati personali del segnalante, in quanto l'indicazione nel verbale dei dati dell'interessato e di quelli dell'altro trasgressore era giustificata dall'esigenza di consentire allo stesso un'eventuale impugnativa del provvedimento sanzionatorio. Il caso integrava infatti una fattispecie di concorso di persone nell'illecito amministrativo e pertanto l'utilizzo di un unico verbale, nel quale erano indicate le generalità dei concorrenti nella violazione, era funzionale al loro diritto di difesa in sede di eventuale impugnativa, tenuto conto del valore probatorio di detto verbale (nota 21 ottobre 2011).

In un'altra segnalazione il Garante veniva informato che in una bacheca collocata fuori dai locali di una questura erano stati affissi gli elenchi, comprendenti nomi, cognomi e numeri delle pratiche, delle persone i cui permessi di soggiorno erano pronti per la consegna.

Invitata dall'Autorità ad adottare soluzioni maggiormente rispettose della riservatezza degli interessati, la questura ha comunicato di aver escluso dalla bacheca i nomi e i cognomi degli interessati, lasciando solamente l'indicazione di nazionalità, data di nascita e numero di pratica. Il Garante ha ravvisato nella soluzione adottata un corretto bilanciamento tra il

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

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

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

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

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

6.2.1. Acquisizione di dati da parte delle forze di polizia

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

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

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

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

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

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

In particolare:

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

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

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

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

Accesso diretto

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

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

7. ATTIVITÀ GIORNALISTICA

7.1. MINORI

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

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

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

7.1.1. Vittime di abusi

In due casi nei quali alcuni quotidiani, nel riferire dell'avvio di un'indagine su presunti abusi sessuali ai danni di una minorenne, avevano diffuso dati ritenuti idonei ad identificarla indirettamente, l'Autorità ha ribadito che non si possono pubblicare dettagli che rendono identificabili vittime di violenza sessuale, tanto più se si tratta di minori. Pertanto, anche i nomi dei violentatori non possono essere diffusi se rendono identificabile la vittima. In particolare, i quotidiani avevano indicato il legame parentale che legava la minorenne con l'indagato, individuato nominativamente, unitamente ad altre informazioni relative alla famiglia, nonché divulgato alcuni dettagli del referto stilato dai medici a seguito degli accertamenti sanitari compiuti sulla bambina. L'Autorità ha rilevato che, anche quando la vittima non viene individuata nominativamente, la diffusione di altre dettagliate informazioni che la riguardino

può comunque renderla riconoscibile, in particolare nella cerchia delle relazioni sociali degli interessati e ciò costituisce una violazione del codice di procedura penale (art. 114, comma 6, c.p.p.), del codice di deontologia per l'attività giornalistica (art. 7) e della Carta di Treviso (comunicati stampa 16 luglio [doc. *web* n.1823757] e 4 agosto 2011 [doc. *web* n. 1828618]).

7.2. CRONACHE GIUDIZIARIE E VITTIME DI REATO

L'Autorità ha risposto a diversi reclami e segnalazioni richiamando il principio, ormai consolidato, secondo cui la pubblicazione di dati personali relativi a procedimenti penali è ammessa anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 5, 6 e 12 del codice di deontologia). La valutazione deve essere fatta caso per caso, in prima battuta dal giornalista, nel quadro anche delle disposizioni che disciplinano il segreto delle indagini e il regime di pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.).

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

7.2.1. Truffa dei Parioli

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

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

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

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

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

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

7.3.1. Diffusione di un documentario su una raffineria sarda

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

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

7.4. DATI SULLA SALUTE

Anche nel periodo di riferimento, come nel passato, si è reso necessario un richiamo al rispetto delle disposizioni che tutelano la riservatezza e la dignità di persone malate, sia da parte delle strutture sanitarie che forniscono informazioni sui loro pazienti, sia da parte degli organi di informazione che accedono a tali informazioni (art. 83 del Codice, artt. 9, 10, 11 e 31 del codice di deontologia medica; art. 10 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica).

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

Il Garante ha avuto altresì occasione di ricordare che la tutela della riservatezza e della dignità di una persona malata non viene meno neanche dopo il suo decesso, in particolare nei casi di suicidio (nota 22 settembre 2011).

7.5. ARCHIVI STORICI E INFORMAZIONI *ONLINE*

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

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

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

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

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

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

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

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

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

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

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

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

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

8. TRATTAMENTO DI DATI PERSONALI ATTRAVERSO INTERNET

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5. I SERVIZI OFFERTI DA MOTORI DI RICERCA

Google Analytics e *Google* Gruppi

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

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

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

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

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

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

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

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

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

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

completo della parola o dell'espressione ricercata, si è attivato al fine di evitare che in tale servizio fosse presente l'associazione, lamentata dal segnalante, che non traeva fondamento alcuno da eventi accertati dall'autorità giudiziaria in capo al segnalante.

Sul servizio *Google Suggest* si è pronunciato anche il Tribunale di Milano (ordinanza 24 marzo 2011), a favore di un imprenditore che vedeva il suo nome associato all'aggettivo "truffatore", imponendo al motore di ricerca in questione di filtrare alcuni suggerimenti ritenuti calunniosi.

8.6. *FACEBOOK*

In misura superiore rispetto all'anno precedente, nel 2011 sono pervenute segnalazioni che lamentavano il trattamento illecito di dati personali su *Facebook*.

L'Ufficio in alcuni casi ha contattato la società *Facebook*.

In particolare ha chiesto informazioni in relazione alla lamentata disattivazione, operata unilateralmente dalla società americana, del profilo dall'interessato. In tale occasione *Facebook* ha sostenuto che il segnalante aveva commesso una violazione delle condizioni contrattuali (nota 7 luglio 2011).

In altri casi, l'Ufficio si è invece rivolto direttamente agli stessi utenti, in particolare con riferimento alle segnalazioni di genitori separati, che lamentavano l'inserimento da parte dell'altro genitore nel proprio profilo *Facebook* di una foto del figlio, in assenza del consenso del genitore segnalante.

In tali ipotesi il Garante ha compiuto una valutazione in concreto caso per caso, assumendo come criteri di riferimento –in una prospettiva di tutela del preminente interesse del minore– il tipo di immagine inserita su *Facebook* e il grado di apertura del profilo nel quale era stata inserita (note 2 febbraio e 3 maggio 2011).

8.7. LA PROTEZIONE DEL DIRITTO D'AUTORE IN RETE: IL CASO FAPAV

Nel periodo di riferimento, l'Autorità ha proseguito l'esame della complessa questione concernente la presunta attività di monitoraggio del traffico telematico degli utenti di Telecom Italia S.p.A., effettuata da Fapav - Federazione antipirateria audiovisiva.

Al riguardo, il Garante aveva ricevuto due segnalazioni agli inizi del 2010 (dalla società Telecom Italia e dall'associazione di consumatori Altroconsumo), dopo che Fapav si era rivolta al Tribunale civile di Roma, lamentando una presunta illecita acquisizione tramite la rete internet di opere audiovisive protette.

In particolare, Fapav aveva evidenziato che ben più della metà dei casi di messa a disposizione e riproduzione di opere audiovisive protette era avvenuta utilizzando la rete di Telecom, alla quale Fapav aveva chiesto, in particolare, di disattivare e/o bloccare l'accesso ai siti attraverso i quali avveniva l'illecita riproduzione, e di comunicare alle autorità di pubblica sicurezza i dati idonei a consentire l'adozione delle misure di competenza. Di fronte al diniego di Telecom, Fapav si era poi rivolta al Tribunale, instaurando il suindicato giudizio, nel quale il Garante si è costituito in conformità alle proprie competenze istituzionali.

Con ordinanza del 15 aprile 2010, il Tribunale ha escluso che, al fine di individuare eventuali violazioni del diritto di autore, il giudice civile possa ordinare ad una società di monitorare la navigazione in rete dei propri utenti, acquisendo dati anche sui siti visitati. Ciò, conformemente con quanto disposto dal Garante in diversi provvedimenti, uno dei quali adottato proprio nei confronti di Telecom.

Durante lo svolgimento della causa civile, il Garante aveva dato inizio agli accertamenti di rito, richiedendo a Fapav di comunicare le modalità tecniche con le quali, anche avvalendosi dell'attività di terzi, erano stati acquisiti i dati personali dei soggetti coinvolti (ossia, i clienti di Telecom) quali gli indirizzi IP, gli *URL* dei siti visitati, la data e l'ora delle connessioni, i file scambiati, ecc.

Nell'ambito del procedimento amministrativo, Fapav ha fornito soltanto i primi riscontri, rifiutandosi poi di far conoscere gli ulteriori e specifici elementi ritenuti necessari dall'Autorità per la conclusione del procedimento stesso. Con ricorso del 3 giugno 2010, Fapav ha, anzi, impugnato dinanzi al Tribunale di Roma anche la richiesta di informazioni, sulla base della considerazione che le informazioni acquisite avrebbero potuto essere utilizzate dal Garante a proprio favore nelle fasi successive del giudizio dinanzi al Tribunale o che di esse si sarebbe potuta giovare Telecom.

Il Garante ha quindi sospeso il procedimento, in attesa della decisione del Tribunale nella causa civile, conclusasi poi con la sentenza del 23 settembre 2011, che ha rigettato il ricorso di Fapav.

Nonostante ciò, alle due successive nuove richieste di informazioni del Garante (che reiteravano sostanzialmente le precedenti rimaste senza risposta) la Federazione ha dapprima, nel novembre 2011, opposto un ulteriore rifiuto di fornire gli elementi richiesti e poi, nel gennaio 2012, informato l'Autorità di aver proposto, avverso le istanze, nuovo ricorso al Tribunale di Roma.

In questo contesto il procedimento amministrativo resta sospeso, e, in termini più generali, rimane aperto il dibattito, anche parlamentare, sul tema della protezione in rete del diritto d'autore.

9. TRATTAMENTO DI DATI PERSONALI NEL SETTORE DELLE TELECOMUNICAZIONI

9.1. LE CHIAMATE INDESIDERATE PROMOZIONALI DOPO L'INTRODUZIONE DEL REGISTRO PUBBLICO DELLE OPPOSIZIONI

Si è riferito nella Relazione 2010 (p. 9 e ss.) dell'istituzione del Registro pubblico delle opposizioni e dei relativi provvedimenti del Garante.

Sono pervenute al riguardo numerosissime segnalazioni (n. 2162 alla data del 29 febbraio 2012), relative a chiamate telefoniche indesiderate giunte sia ad utenze pubblicate negli elenchi telefonici ed iscritte nel Registro pubblico delle opposizioni, sia ad utenze riservate, i cui intestatari hanno rappresentato di sentirsi privi anche di una forma minima di tutela, in quanto impossibilitati ad iscriversi allo stesso Registro.

Nella maggior parte dei casi è stata lamentata la ricezione di più telefonate promozionali, effettuate anche da soggetti diversi, per oltre 4000 violazioni complessive, con un flusso di segnalazioni che si è mantenuto costante nei vari mesi.

Per ogni presunta violazione è stata avviata una specifica istruttoria preliminare. La fase di avvio dell'attività è stata caratterizzata da alcune difficoltà operative sia per l'elevato numero di segnalazioni, sia per la necessità di contattare gli interessati al fine di acquisire gli elementi necessari per poter procedere, quali il numero chiamato e –ove conosciuto– il numero chiamante. In alcuni casi, la mancata conoscenza di quest'ultimo dato è dipesa dal fatto che l'interessato non disponeva dello specifico dispositivo che consente di visualizzare i numeri in ingresso sul display del proprio terminale; in altri casi, invece, quel numero è stato volutamente "oscurato" e dunque reso anonimo dal chiamante stesso, in violazione dell'obbligo stabilito dall'art. 9 del d.P.R. 7 settembre 2010, n. 178.

Alla luce degli inconvenienti riscontrati, l'Autorità ha reso disponibile sulla home page del proprio sito un modello di agevole compilazione, da completare con tutti gli elementi necessari per l'istruttoria, allo scopo di segnalare all'Autorità la ricezione di telefonate pubblicitarie non richieste.

In molti casi l'Autorità è riuscita a identificare la linea chiamante sia in Italia sia all'estero, e sono stati avviati specifici accertamenti al fine di verificare la liceità del trattamento.

Al riguardo, è emerso che talvolta il contatto promozionale era avvenuto in data successiva all'iscrizione dell'utenza nel Registro delle opposizioni, ma prima dello scadere del termine di 15 giorni previsto dall'art. 8, comma 2, del d.P.R. n. 178/2010.

In un numero significativo di casi, inoltre, è stato accertato che il segnalante aveva fornito, a volte in tempi risalenti e nelle occasioni più varie, un consenso alla ricezione di contatti pubblicitari specifico o più spesso generalizzato e dunque relativo anche ai trattamenti con finalità commerciali effettuati da terzi (spesso all'atto della compilazione di coupon o nel corso della partecipazione a concorsi a premi o, ancora, in occasione di sondaggi ecc.), salvo poi non serbarne memoria, perdendo così qualsiasi possibilità di controllo sui trattamenti di dati che lo riguardano. In altre occasioni il consenso era stato fornito non dall'intestatario della linea, ma da un terzo, suo convivente ed utilizzatore dell'utenza telefonica, magari all'insaputa dell'intestatario stesso.

In tutti questi casi i contatti oggetto di doglianza sono risultati legittimi e, pertanto, non si è instaurato alcun procedimento sanzionatorio; il titolare del trattamento ha però preso atto dell'opposizione manifestata, per il tramite della segnalazione, dall'interessato.

Anche alla stregua dei dati forniti, sulla base di un primo parziale bilancio dell'attività –anche a carattere sanzionatorio– condotta dal Garante nel primo anno dall'entrata in vigore delle norme in materia di Registro delle opposizioni, si può affermare che il nuovo sistema non ha finora conseguito risultati apprezzabili in termini di efficacia: rispetto ai dati dell'anno precedente, si è infatti registrata una forte crescita nel numero delle segnalazioni, in termini che palesano un crescente livello di irritazione dei cittadini.

Passando ad altro profilo, si evidenzia che alcuni operatori hanno ritenuto eccessivamente onerosi i costi di accesso al Registro, riportati nella tabella di cui all'art. 2, comma 1, del d.m. 22 dicembre 2010. Il Garante ha segnalato tali valutazioni al Ministro dello sviluppo economico che, dal 1° gennaio 2012, ha sensibilmente ridotto le tariffe.

Registro delle opposizioni e telefonate senza *calling line identification (cli)*

Il Garante è intervenuto anche per reprimere il fenomeno delle telefonate effettuate senza *calling line identification* (*cli*), adottando in data 23 febbraio 2012 tre provvedimenti di blocco del trattamento dei dati nei confronti di altrettante società operanti nel settore del *telemarketing* [doc. *web* nn. 1877065, 1877080 e 1878559].

Tali società –che forniscono servizi di *call center* per promuovere prodotti e servizi di altre aziende– non solo effettuavano chiamate pubblicitarie indesiderate ad utenze iscritte nel Registro delle opposizioni, ma non rendevano identificabile la linea chiamante, impedendo in tal modo agli abbonati di tutelare i loro diritti, benché sia espressamente vietato ai soggetti che effettuano chiamate commerciali e promozionali di camuffare o celare la loro identità (v. art. 130, comma 5, del Codice).

Alla luce di queste violazioni, il Garante ha dichiarato illecito il trattamento dei dati effettuato dalle tre società e ne ha disposto il blocco, impedendo l'uso dei dati raccolti fino a quando esse non abbiano regolarizzato la propria posizione e inviato all'Autorità la documentazione comprovante l'avvenuto adeguamento. Il Garante inoltre si è riservato di valutare la possibilità di applicare a tali società la sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, del Codice.

Con i medesimi provvedimenti è stata disposta –in una prospettiva di tutela quanto più possibile ampia ed effettiva degli interessati iscritti al Registro delle opposizioni– l'apertura di autonomi procedimenti amministrativi nei confronti delle società che si sono avvalse dei servizi dei tre *call center*, per accertare la liceità dei trattamenti dati svolti.

Alla luce della nuova disciplina, l'Autorità ha anche evidenziato che non è più necessario indicare negli elenchi telefonici, tramite l'apposito simbolo grafico, il consenso alla ricezione di chiamate telefoniche a carattere promozionale. Per agevolare il completo adeguamento alle nuove prescrizioni l'Autorità ha concesso, a seguito dell'istanza presentata da Asstel-Assotelecomunicazioni, una proroga dei termini previsti per l'adozione dei nuovi modelli di informativa e consenso (provv. 5 maggio 2011, in G.U. 18 maggio 2011, n. 114 [doc. *web* n. 1811916]) e, dopo la scadenza del termine già prorogato, ha svolto, anche a seguito delle numerose comunicazioni pervenute, una specifica attività di monitoraggio, volta a verificare l'effettiva adozione da parte degli operatori delle misure previste.

Tutela delle utenze riservate

In relazione alle numerose segnalazioni relative a telefonate promozionali indesiderate ad utenze riservate, senza l'acquisizione del consenso informato richiesto dagli artt. 13 e 23 del Codice, l'Autorità, con un provvedimento inibitorio e prescrittivo, ha vietato ad un importante gestore telefonico, anche per il tramite di propri agenti, il trattamento di qualunque dato

personale correlato all'effettuazione di telefonate promozionali con operatore su utenze riservate, senza l'acquisizione del necessario consenso, imponendo ad esso l'adozione di tutte le misure necessarie a garantire la completa osservanza della disciplina in materia di protezione dei dati personali (provv. 21 luglio 2011 [doc. *web* n. 1832551]).

Utenze tratte da albi professionali

Il Garante ha inoltre ribadito i limiti del trattamento dei dati personali nell'ambito del *telemarketing* chiarendo, in linea con quanto precisato nel provvedimento del 19 gennaio 2011 [doc. *web* n. 1784528], che i dati contenuti in un registro, elenco o albo consultabile da chiunque possono essere utilizzati per telefonate commerciali solo se il promotore abbia già acquisito il consenso dell'interessato o se presenti offerte strettamente attinenti all'attività svolta dal soggetto contattato.

Su tali basi è stato dichiarato illecito il trattamento svolto attraverso telefonate promozionali con operatore, utilizzando il recapito telefonico di un avvocato, tratto dal relativo albo professionale *online*, per offerte commerciali generiche non "direttamente funzionali" alla professione forense e che non giustificavano l'eventuale esonero dall'acquisizione del consenso (provv. 29 settembre 2011 [doc. *web* n. 1851415]).

9.2. TITOLARITÀ DEL TRATTAMENTO IN CAPO A CHI SI AVVALE DI AGENTI PER IL *MARKETING*

Al fine di chiarire i ruoli dei soggetti che operano nel settore del *telemarketing* l'Autorità ha adottato il provvedimento generale del 15 giugno 2011 [doc. *web* n. 1821257], prorogando poi i termini per l'adempimento delle prescrizioni ivi contenute (provv. 7 settembre 2011 [doc. *web* n. 1839211]).

In sintesi, al ricorrere di determinate condizioni, le società che si avvalgono di agenzie o altre imprese in *outsourcing* per la promozione e la commercializzazione dei propri prodotti o servizi non possono che essere considerate titolari del trattamento dei dati dei potenziali clienti, anche quando tale titolarità risulti formalmente in capo agli *outsourcer*.

A tal fine, più che l'aspetto formale deve essere valutato l'atteggiarsi effettivo dei rapporti. Pertanto, il soggetto in nome o per conto del quale venga effettuata l'attività promozionale che agisca, di fatto, come titolare, ossia –come accade frequentemente nella pratica– definisca obiettivi, strategie commerciali ed istruzioni, elargendo incentivi agli *outsourcer* in base ai

risultati raggiunti e predisponendo la modulistica necessaria, dovrà anche rispondere di eventuali illeciti. Per queste ragioni, il Garante ha prescritto che le società che affidano all'esterno l'attività di promozione ma ne mantengono di fatto il controllo operativo, e quindi si configurano come titolari del trattamento dati, siano tenute anche a designare formalmente responsabili del trattamento i promoter o gli agenti di cui si avvalgono.

9.3. IL PROVVEDIMENTO SULLE TELEFONATE "MUTE"

Con il provvedimento del 6 dicembre 2011 [doc. *web* n. 1857326], il Garante ha adottato un primo intervento per contrastare il fenomeno delle cosiddette telefonate "mute", nelle quali il destinatario, dopo aver sollevato il ricevitore, non viene messo in comunicazione con alcun interlocutore.

Le segnalazioni pervenute hanno rappresentato che la ricezione di questo tipo di chiamate, reiterata a volte anche nell'arco della medesima giornata e spesso protratta nel tempo, ha cagionato un notevole disturbo ai destinatari ai quali, in difetto appunto di interlocutore, sono stati preclusi tutele e rimedi.

Tale fenomeno nasce dalla scelta di alcuni operatori di *telemarketing* di telefonare tramite un sistema automatizzato, il quale consente di scegliere il numero dei potenziali contatti da instaurare, tenuto conto di diversi parametri, tra i quali il numero degli addetti concretamente impegnati nello specifico *call center* in un dato momento. Un singolo *teleseller* può, cioè, richiedere al sistema l'effettuazione e l'inoltro di un numero di telefonate anche di molto superiore alla propria capacità ricettiva e di lavorazione, con l'intento di assicurarsi che i propri operatori, al termine di ciascuna telefonata effettuata, ne abbiano sempre a disposizione una ulteriore, già instradata ed attivata, da prendere in carico ed evitare, così, che rimangano inattivi o si ingenerino tempi morti, trasferendo di fatto tempi e costi di attesa sul soggetto chiamato. L'effetto è tuttavia che non per ogni telefonata inoltrata ci sia un operatore disponibile e pertanto in tali ipotesi il destinatario della comunicazione riceve appunto una telefonata "muta" (in gergo tecnico si parla di un contatto cd. "abbattuto" il quale peraltro, non essendo andato a buon fine, è potenzialmente reiterabile).

Al riguardo, l'Autorità, al termine di una lunga istruttoria, ha prescritto alla società che si avvaleva di questo sistema una serie di misure e di accorgimenti per impedire la reiterazione di telefonate mute ed escludere la possibilità di richiamare il numero in questione per almeno trenta giorni.

9.4. *MOBILE MARKETING* E *DIRECT E-MAIL MARKETING*

Nell'ambito del *direct marketing*, anche nel 2011, il Garante si è occupato, delle attività promozionali svolte mediante *database* contenenti numeri di utenze telefoniche mobili, sulla base di numerosi accertamenti, anche di natura ispettiva, avviati già nel 2010.

I settori di attività nei quali sono risultate operanti le società sottoposte ad accertamento sono piuttosto variegati. Oltre a quello riconducibile all'invio di messaggi promozionali tramite sms (cd. "*mobile marketing*" o "*sms advertising*") o tramite e-mail (cd. "*direct e-mail marketing*" o *DEM*), oggetto diretto degli accertamenti svolti, le società ispezionate si occupano anche di: pubblicazione di contenuti sul *web*; fornitura di servizi a valore aggiunto (cd. "VAS"); commercializzazione di loghi e suonerie e altri contenuti per telefoni mobili; registrazione di nomi a dominio; attività di *provider* di servizi di posta elettronica; creazione di spazi internet per la pubblicazione di blog.

Con riguardo alle attività di *mobile marketing* e *DEM*, dagli accertamenti è emerso che, nella maggior parte dei casi, le società ispezionate sono dotate di un proprio *database* di numeri di telefoni mobili o di indirizzi di posta elettronica ai quali inviare i messaggi promozionali. Vi sono tuttavia anche società che svolgono un ruolo di intermediazione tra chi vuole effettuare campagne di *marketing* e chi detiene i *database* e che non hanno nessun contatto con i dati personali verso i quali vengono indirizzati i messaggi stessi.

Si è potuto verificare tuttavia come ciò non determini necessariamente una maggiore garanzia di sicurezza per i dati personali degli interessati, in quanto la presenza di intermediari e l'impossibilità che, a monte delle attività di *marketing*, vi sia un soggetto deputato al coordinamento delle stesse, rendono complicato l'esercizio dei diritti riconosciuti agli interessati e li espongono (nel caso in cui i dati personali siano registrati su più *database*) al rischio di numerose comunicazioni indesiderate aventi identico tenore.

In alcuni casi è emerso invece che gli intermediari accedono ai *database* contenenti i dati dei destinatari delle attività promozionali e che le relative comunicazioni di informazioni personali non sono sempre conformi alla normativa in materia di *privacy*. Ciò, con riguardo agli adempimenti concernenti l'informativa e il consenso degli interessati ovvero al profilo della distribuzione delle responsabilità nell'ambito del trattamento e, quindi, alle nomine di soggetti esterni quali responsabili o incaricati del trattamento.

In merito alle specifiche modalità con le quali vengono forniti i servizi di *marketing*, si è accertato che normalmente sono le società del settore –ricevuto l'incarico di effettuare la campagna promozionale– ad inviare il relativo messaggio (via sms o e-mail) alle numerazioni o agli indirizzi di posta elettronica presenti nel *database* di cui dispongono. Vi sono però anche società che offrono *online* piattaforme informatiche tramite le quali chi intende effettuare una campagna promozionale può procedere direttamente agli invii dei messaggi, senza accedere ai dati personali dei destinatari, ma semplicemente inserendo negli appositi campi il testo del messaggio da inviare e le caratteristiche che debbono avere i destinatari dello stesso. Il sistema seleziona poi la platea di destinatari che presenta i requisiti indicati dal cliente ed inoltra i messaggi promozionali.

Nel 2011 sono state chiuse istruttorie nei confronti di tredici società. Nei cinque casi in cui l'Ufficio ha accertato l'illiceità del trattamento effettuato dalla società e/o la non conformità dell'attività svolta rispetto alla normativa in materia di protezione dei dati personali, sono stati adottati altrettanti provvedimenti del Garante di natura inibitoria e/o prescrittiva (cfr. provv.ti 10 giugno 2011 [doc. *web* n. 1836396]; 30 giugno 2011 [doc. *web* n. 1834208]; 15 settembre 2011 [doc. *web* n.1849872]; 26 ottobre 2011 [doc. *web* n.1851750]; 24 novembre 2011 [doc. *web* n.1876435]).

Nei casi in cui, viceversa, non sono stati ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali o, comunque, per promuovere l'adozione di un provvedimento dell'Autorità, ai sensi dell'art. 11 del regolamento del Garante n. 1/2007, si è disposta la conclusione del procedimento amministrativo.

Sotto il profilo sanzionatorio, sono stati avviati quattro procedimenti nei confronti di altrettante aziende: in essi, quattro contestazioni hanno riguardato la violazione dell'obbligo

di informativa e cinque la violazione della disciplina relativa al consenso. In tutte le contestazioni è stata ritenuta sussistente l'aggravante prevista dall'art. 164-*bis*, comma 3, del Codice, poiché le condotte hanno coinvolto un numero rilevante di interessati (cfr. par. 17.).

9.5. *NUMBER PORTABILITY*: TRATTAMENTO DEI DATI DEGLI ABBONATI PRESENTI NEGLI ELENCHI TELEFONICI

Riguardo al trattamento dei dati personali degli abbonati presenti negli elenchi telefonici in caso di *number portability*, con provvedimento del 7 luglio 2011 (in G.U. 1° agosto 2011, n. 177 [doc. *web* n. 1824538]), l'Autorità ha dato seguito alle richieste presentate dagli operatori circa l'attuazione, del provvedimento del Garante del 1° aprile 2010 [doc. *web* n. 1824538] che stabiliva il principio del mantenimento del consenso dell'abbonato al trattamento dei propri dati personali, già espresso e registrato nel cd. *database* unico degli abbonati (DBU) anche nel caso di portabilità del numero, salvo la comunicazione al nuovo operatore di una diversa scelta dello stesso.

Il Garante ha valutato le difficoltà di natura tecnica rappresentate in merito all'obbligo di tutti gli operatori di telefonia fissa e mobile di acquisire, con continuità, i consensi già rilasciati dagli abbonati di altri operatori in caso di *number portability* (a causa della cancellazione automatica dei consensi in caso di cessazione del contratto con l'operatore originario) e concesso una sospensione dell'efficacia del citato provvedimento sino alla data del 1° novembre 2011.

L'Autorità ha così consentito a tutti gli operatori del mercato, soprattutto a quelli di piccole dimensioni che avevano rappresentato una serie di difficoltà tecniche nella "lettura del DBU", di pervenire alla definitiva implementazione di tutte le funzionalità, idonee a garantire, anche attraverso un apposito *software* fornito dall'Iscom (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione), la piena attuazione delle prescrizioni precedentemente dettate con il citato provvedimento del 1° aprile 2010.

9.6. ELENCHI TELEFONICI *ONLINE*

In numerose segnalazioni e reclami è stata lamentata la diffusione sul sito *web* di una società di un elenco telefonico *online* contenente vari dati (nome e cognome, indirizzo,

recapito telefonico, numero della partita IVA) degli interessati, alcuni peraltro di carattere "riservato". La procedura per l'eliminazione dei dati degli interessati dal menzionato elenco telefonico richiedeva preliminarmente la registrazione a tale sito.

Dall'accertamento condotto è emerso che la società possedeva una "banca dati *online*", relativa a persone fisiche e ad imprese, alimentata sia mediante elenco telefonico digitale, fornito da un primario operatore telefonico, sia mediante registrazione di nuovi utenti visitatori del sito.

Al riguardo l'Autorità ha ritenuto illecito il trattamento di dati personali effettuato tramite la costituzione e diffusione *online* di un elenco telefonico se i dati personali contenuti non sono stati tratti dal DBU. Ha altresì affermato che un elenco telefonico basato su una fonte diversa dal DBU non può essere utilizzato per la funzione di "ricerca inversa", ossia per la ricerca del nominativo di un abbonato sulla base del suo numero telefonico, rilevando inoltre la mancanza di un consenso espresso dell'interessato a tale funzione (provv. 7 aprile 2011 [doc. *web* n. 1810351]).

9.7. IL PARERE SULLA COSTITUZIONE DI UNA *BLACK LIST* DEI CLIENTI TELEFONICI MOROSI

Il Garante si è pronunciato, con un parere reso all'Autorità per le garanzie nelle comunicazioni, anche sulla costituzione di *black list* dei clienti telefonici morosi, prospettata dagli operatori telefonici per individuare eventuali morosità dell'utente che richieda la portabilità del numero.

L'Autorità ha ribadito, come già in passato, che la costituzione di banche dati contenenti informazioni negative sullo stato di solvibilità dell'utente richiede una precisa fonte normativa che specifichi, oltre alla possibilità di raccogliere i dati senza il consenso dell'interessato, anche la finalità perseguita, i soggetti che possono accedervi e le modalità di consultazione.

Tali elementi possono essere individuati anche tramite rinvio da parte della norma ad una fonte di rango secondario (come i regolamenti, in tal caso, soggetti alla previa acquisizione del parere del Garante) o ai codici di deontologia e buona condotta (da adottare secondo i procedimenti previsti).

In tal senso, l'Autorità ha ricordato l'esistenza, nel settore del credito al consumo, di banche dati contenenti informazioni relative a coloro che chiedono di accedere a prestiti, mutui o finanziamenti, sulla base della specifica normativa contenuta nell'art. 117 del Codice, che prevede la sottoscrizione di un "codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti".

Il Garante ha poi precisato che la formazione di una banca dati dei "cattivi pagatori", senza una specifica previsione contrattuale, può comportare una rilevante modifica del tradizionale rapporto negoziale tra le parti, nonché generare abusi e rischi di discriminazione ed avere serie ripercussioni sulla vita delle persone.

L'Autorità ha altresì evidenziato le difficoltà della costituzione di una simile black list senza l'utilizzo di informazioni personali sui clienti, come invece ipotizzato dagli operatori telefonici, posto che anche la sola indicazione del numero telefonico dell'abbonato moroso consente di risalire alla relativa identità. Del resto, la prospettata procedura di accesso al *database* attraverso lo scambio di informazioni sulla morosità unicamente tra il vecchio operatore telefonico (cd. *"donating"*) e quello nuovo (cd. *"recipient"*) diversamente da quanto sostenuto dagli operatori, configurerebbe una comunicazione di dati che richiederebbe un'adeguata informativa e l'acquisizione del consenso (parere 27 ottobre 2011).

9.8. TELEFONIA: RACCOLTA DI DATI PERSONALI MEDIANTE I MODULI CONTRATTUALI

Numerose segnalazioni relative all'attività di un importante operatore telefonico, che svolge attività di fornitura di vari servizi di comunicazione elettronica (es.: trasmissione dati, fonia, *housing*, ecc.), hanno lamentato l'effettuazione di telefonate promozionali indesiderate nonché l'attivazione non richiesta di un'utenza telefonica e del servizio di *carrier preselection* (che consente all'utente di scegliere un operatore diverso da quello con il quale ha già un contratto, trasferendo il proprio traffico telefonico sulla rete dell'operatore prescelto alle condizioni contrattuali con quest'ultimo pattuite).

L'Autorità, con apposita attività ispettiva, ha accertato che l'attivazione del servizio di *carrier preselection* era avvenuta mediante moduli contrattuali utilizzati fin dal giugno 2007 e

già sottoscritti da migliaia di clienti (sia consumatori sia imprese pubbliche e private), che non prevedevano l'espressione del consenso libero, specifico e documentato per iscritto degli interessati, in relazione ad attività diverse da quelle strumentali all'esecuzione degli obblighi contrattuali (cfr. artt. 23 e 130 del Codice). Sulla base della documentazione acquisita, l'Autorità ha dichiarato illecito e inibito il trattamento di dati personali raccolti mediante i moduli utilizzati per il servizio di carrier preselection ovvero per qualsiasi altro servizio fornito dalla società in questione (provv. 12 gennaio 2012 [doc. *web* n. 1884254]).

9.9. LA LOTTA ALLO *SPAM*

Anche nel 2011 il Garante ha ricevuto numerose richieste d'intervento relative ad attività di *spam* realizzata mediante diversi mezzi (posta elettronica, fax, chiamate telefoniche preregistrate, sms).

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

Riguardo alle specifiche modalità di trattamento, anche nel 2011, il fax e l'e-mail sono stati i mezzi più utilizzati per le attività di *spam*.

Rimangono numerose le violazioni, soprattutto via e-mail, per le quali talora risulta difficile individuare il titolare del trattamento, sia per le modalità con cui si può operare in rete, sia perché spesso i titolari hanno sede in Paesi extraeuropei ove l'Autorità non ha competenza.

Fax indesiderati

In più occasioni, è stato vietato l'invio mediante telefax di comunicazioni promozionali a terzi, in assenza di informativa e consenso preventivo, specifico e documentato degli interessati, ai sensi degli artt. 13, 23 e 130 del Codice.

Il Garante ha in particolare ricordato che i soggetti che acquisiscono banche dati da terzi devono previamente accertare che ciascun interessato abbia validamente acconsentito all'utilizzo dei propri dati ai fini di invio di materiale pubblicitario, a pena di illiceità del trattamento (v., tra gli altri, provv. 26 gennaio 2011 [doc. *web* n. 1790397]).

Si evidenzia in materia, inoltre, il provvedimento inibitorio e prescrittivo adottato il 2 marzo 2011 [doc. *web* n. 1842423], dopo apposita ispezione, nei confronti di una società che gestiva tre siti *web* sprovvisti dell'informativa richiesta dall'art. art. 13 del Codice.

In questo caso, il Garante ha ricordato che i soggetti che acquisiscono dati da terzi devono accertare che ciascun interessato abbia validamente acconsentito all'utilizzo dei propri dati ai fini di invio di materiale pubblicitario poiché, come già stabilito nel provvedimento 29 maggio 2003 [doc. *web* n. 29840], relativo allo *spamming*, non ha rilievo che i medesimi dati siano già reperibili altrove; v. provv. 3 febbraio 2011 [doc. *web* n. 1792588] e Relazione 2010, p. 125). Pertanto l'Autorità, oltre ad inibire l'invio di fax indesiderati, ha prescritto di modificare l'informativa *ex* art. 13 del Codice, con l'indicazione delle modalità e delle finalità del trattamento svolto dalla società in questione.

Collegato a tale provvedimento è quello adottato nei confronti di un'altra società, pubblicizzata in uno dei tre siti sopra menzionati quale leader di mercato per il servizio di messaggistica fax/e-mail/sms (provv. 5 maggio 2011 [doc. *web* n. 1822815]).

È emerso che tale società talora offriva ai clienti un servizio di invio di messaggi, mediante i propri operatori, a liste di destinatari, estrapolati da un *database* collocato sul proprio *server*, contenente dati personali (ragione sociale e numerazione telefonica cui inviare i fax e/o indirizzo e-mail) di circa tredicimila imprese (agenzie di viaggio e *tour operator*).

In proposito, l'Autorità ha fatto riferimento all'art. 13, comma 4, del Codice, in base al quale, se i dati personali non sono raccolti presso l'interessato, l'informativa va data al medesimo interessato all'atto della registrazione dei dati.

Inoltre, ha prescritto alla società in questione –similmente a quanto disposto con il provvedimento del 7 aprile 2011 [doc. *web* n. 1810207], di cui più diffusamente *infra*– qualora intenda continuare a fornire il servizio di invio di comunicazioni promozionali con modalità automatizzate, di adottare tutte le misure necessarie a garantire agli interessati la possibilità di esercitare agevolmente i diritti di cui all'art. 7 del Codice. In particolare, ha richiesto che per ogni messaggio in uscita sia predisposto un riquadro (*template*) recante un'idonea informativa, comprendente un recapito presso cui l'interessato possa esercitare tali diritti.

Infine, nei casi in cui si è accertato che l'invio di fax indesiderati era stato effettuato da società localizzate all'estero (Francia, Regno Unito e Romania), è stata richiesta la collaborazione delle competenti autorità straniere per far cessare tali invii.

Mail *spamming*

Princìpi analoghi a quelli sin qui richiamati sono stati ribaditi in materia di e-mail indesiderate, con il provvedimento inibitorio e prescrittivo adottato nei confronti della società titolare di un sito *web* mediante il quale venivano raccolti dati personali utilizzati, oltre che per l'invio della *newsletter* richiesta, per trattamenti diversi, quali l'inoltro di messaggi promozionali propri o di altri soggetti e la comunicazione dei medesimi dati a società specializzate nel *marketing* e nelle ricerche di mercato (provv. 19 maggio 2011 [doc. *web* n. 1823148]). Tuttavia non veniva acquisito un consenso specifico per questi tipi di trattamento e si consentiva all'utente interessato di registrarsi al sito solo accettando integralmente quanto riportato nell'informativa sul trattamento dei dati.

Il Garante ha pertanto vietato sia il trattamento dei dati personali effettuato tramite l'invio di e-mail promozionali agli utenti registrati per la ricezione delle *newsletter* del sito in questione, sia la comunicazione dei dati acquisiti a soggetti terzi, per finalità di ricerche di mercato e di comunicazione commerciale, in assenza di un consenso libero, specifico e documentato per iscritto degli interessati *ex* artt. 23 e 130 del Codice. Inoltre, alla società è stato prescritto di inserire –in fase di registrazione– la richiesta agli interessati di un preventivo consenso distinto e facoltativo per ciascuna finalità indicata nell'informativa da fornire agli utenti *ex* art. 13 del Codice.

Spam diretto ad utenze mobili

Si segnala che, nell'ambito della complessa attività di contrasto allo *spamming*, il Garante ha verificato che vi fossero i presupposti per ritenere illecita l'attività di contatto, da parte di una nota società di finanziamento, dell'utenza mobile di diversi soggetti che non avevano prestato il proprio consenso alla ricezione di messaggi di carattere promozionale e che avevano successivamente manifestato, senza ottenere riscontro, la propria opposizione al trattamento (nota 2 marzo 2011).

Nel ribadire l'esigenza di rispettare le disposizioni in materia di consenso e di comunicazioni indesiderate, (artt. 23 e 130 del Codice), l'Autorità ha anche chiarito come il titolare del trattamento dei dati, al fine di garantire l'effettivo esercizio dei diritti di cui all'art. 7 del

Codice, sia tenuto a predisporre idonee misure organizzative che consentano l'esercizio stesso, attraverso modalità semplici e non onerose per l'interessato.

Spam proveniente dall'estero

L'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei, in termini sia di disciplina sostanziale, sia di tutele garantite dall'ordinamento giuridico, in relazione alla veste giuridica dei destinatari delle comunicazioni promozionali automatizzate indesiderate (per le disposizioni che hanno in buona misura escluso dall'ambito di applicazione del Codice le persone giuridiche v. d.l. n. 201/2011, convertito dalla l. n. 214/2011; v. par. 2.1.1.).

In tema di illecito trattamento dati mediante l'invio di fax, l'Autorità si è pronunciata nei confronti di una società che, sebbene conservasse all'estero i dati personali e li gestisse in modalità remota, utilizzava in modo prevalente e per le funzioni più importanti un apparato di rete (fax *gateway*) collocato sul territorio italiano. Per tale ragione, il Garante ha ritenuto la società tenuta al rispetto della normativa del Codice e quindi ha dichiarato illecito e inibito l'invio di fax promozionali mediante modalità automatizzate, senza aver fornito un'idonea informativa, senza aver acquisito il consenso dell'interessato, e in assenza di un idoneo recapito per l'esercizio dei diritti di cui all'art. 7 del Codice.

Inoltre, il Garante ha prescritto alla medesima società di predisporre, quale titolare del trattamento, per ogni messaggio in uscita, un riquadro (*template*) recante un'idonea informativa, e di verificare l'esistenza di un consenso preventivo, specifico e informato dei destinatari delle suddette comunicazioni promozionali.

L'Autorità ha inoltre ravvisato nel trattamento dati effettuato, la configurabilità –oltre che delle violazioni amministrative concernenti l'omesso rilascio dell'informativa e l'omessa acquisizione del consenso– anche della violazione penale relativa al trattamento illecito di dati (art. 167 del Codice), in ragione del nocumento conseguente all'invio massivo di fax. Il Garante si è altresì riservato di verificare, con autonomi procedimenti, la liceità del trattamento operato dalle singole società committenti individuate nel corso dell'ispezione e dei successivi accertamenti (provv. 7 aprile 2011 [doc. *web* n. 1810207]).

Più in generale, per i casi in cui l'invio di comunicazioni promozionali automatizzato è risultato episodico, l'Autorità ha inviato apposite note di richiamo al pieno rispetto della

disciplina in materia (note 30 novembre 2011 e 7 dicembre 2011) e talora avviato autonomi procedimenti sanzionatori per la contestazione delle sanzioni amministrative previste dagli artt. 161 e 162, comma 2-*bis*, del Codice.

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

Nel 2011 il Garante ha proseguito l'attività ispettiva avviata nel 2010 per la verifica del corretto adempimento, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, delle misure tecnico-giuridiche prescritte con i provvedimenti emanati a seguito delle istanze di *prior checking* da essi presentate all'Autorità, relative all'utilizzo dei dati personali aggregati di traffico telefonico e telematico dei clienti, per finalità di profilazione, senza l'acquisizione del relativo specifico consenso, così come stabilito nel provvedimento generale del 25 giugno 2009 [doc. *web* n. 1629107].

Nell'ambito di tale attività l'Autorità ha riscontrato una serie di irregolarità ed inadempimenti da cui sono scaturiti provvedimenti di blocco dei trattamenti di profilazione, sino alla verifica del puntuale e completo adempimento delle misure prescritte.

In alcuni casi, a fronte degli accertati inadempimenti, sono state anche comminate rilevanti sanzioni amministrative. In altri casi il Garante ha dettato ulteriori misure prescrittive volte a rafforzare la tutela dei soggetti interessati.

Presso gli stessi operatori coinvolti, l'Autorità ha poi dato avvio alla verifica dell'effettiva attuazione di tutte le prescrizioni impartite.

Con riguardo all'attività di profilazione, sono pervenute anche nuove istanze di verifica preliminare che hanno condotto all'emanazione di provvedimenti diretti a consentire tale attività con l'utilizzo di dati aggregati degli utenti, sulla base del previsto esonero dall'acquisizione del consenso, una volta adottate le specifiche misure tecnico-giuridiche dettate dal Garante.

9.11. ISTRUTTORIE SU CASI DI MALFUNZIONAMENTO DI SISTEMI E DI DISPERSIONE DI DATI PERSONALI

Nell'aprile 2011 l'Autorità ha verificato la liceità del trattamento dati effettuato da un'importante società multinazionale mediante dispositivi smartphone/tablet computer, i

quali registrano e conservano nella loro memoria interna dati relativi alla posizione dell'utente nonché alle celle di rete mobile e degli access point Wi-Fi rilevati in prossimità (dato che può indirettamente identificare la posizione dell'utente).

Sul caso, rispondendo ad apposita richiesta di informazioni formulata dall'Autorità, la società ha comunicato di aver reso disponibile, un aggiornamento *software* gratuito che ha risolto diversi dei problemi evidenziati ed originati da un cd. "bug", ed ha aggiunto nuove funzioni correttive idonee a risolvere i problemi lamentati.

Tra il 17 ed il 19 aprile 2011 alcuni sistemi informatici di un grande gruppo societario operante nei settori dell'elettronica di consumo e della comunicazione, relativi ai servizi *online* per clienti, hanno subìto un attacco informatico, con sottrazione dei dati personali di circa 77 milioni di utenti. Il *data-center* ubicato negli USA conteneva parecchi dati della clientela: nome, cognome, indirizzo e-mail, indirizzo postale, data di nascita, sesso, lingua, *online id*, password, domande per il recupero della password nonché l'eventuale numero di carta di credito e la relativa data di scadenza, ma non il codice di sicurezza (CVV).

Nel corso dell'istruttoria, il Garante ha accertato che i clienti italiani coinvolti erano 1,47 milioni e di questi 217.128 avevano fornito il numero della carta di credito. La società non è stata in grado di confermare né escludere che tali dati relativi alle carte di credito fossero stati trafugati, ma ha confermato l'adozione di nuove misure di sicurezza, tecniche e organizzative: lo spostamento dei *server* ad altra sede; l'implementazione di sistemi di sicurezza aggiuntivi come firewall, alert e monitor di attività anomale e intrusioni; l'uso di protezioni crittografiche; l'istituzione della figura del *Chief Information Security Office*. Si è detta, inoltre, disponibile a valutare eventuali, comprovate richieste di risarcimento. Sul caso sono tuttora in corso indagini da parte dell'FBI.

Nell'aprile 2011, un corto circuito in uno dei gruppi di continuità elettrici (batterie dei gruppi UPS) ha causato un principio di incendio presso il *data-center* di un importante internet service *provider* italiano, con conseguente interruzione, per alcune ore, di tutti i servizi informatici erogati. Al riguardo l'Autorità ha condotto appositi accertamenti istruttori dai quali è emerso che non si è comunque verificata alcuna perdita, distruzione o violazione dei dati, come confermato anche dall'assenza di segnalazioni o lamentele degli utenti.

Sempre nel mese di aprile 2011 si è appreso dai mezzi di informazione che la polizia olandese aveva pianificato controlli periodici sui limiti di velocità, ricorrendo a un *database* contenente dati cinematici e di localizzazione di mezzi circolanti sulla rete stradale, fornito indirettamente da una società che produce sistemi di navigazione satellitare. Tale *database*, apparentemente alimentato da dati di geolocalizzazione aggregati trasmessi dai dispositivi di navigazione presenti a bordo di autoveicoli, in alcuni casi sarebbe stato infatti concesso in uso –dietro pagamento di una licenza– a una società intermediaria che, a sua volta, l'avrebbe concesso in licenza alla polizia olandese.

L'istruttoria condotta dal Garante ha evidenziato che i trattamenti dei dati in questione non riguardavano il territorio italiano e, comunque, avvenivano in forma anonima ed aggregata e che l'informativa resa e le formule utilizzate per l'acquisizione del consenso degli interessati erano conformi alle prescrizioni di legge.

10. PROTEZIONE DEI DATI PERSONALI E RAPPORTO DI LAVORO PUBBLICO E PRIVATO

Numerose ed eterogenee sono le segnalazioni indirizzate all'Autorità da parte di lavoratori o di rappresentanze sindacali, ovvero le richieste di datori di lavoro, concernenti il trattamento di dati personali nell'ambito del rapporto di lavoro pubblico e privato. Vi sono tuttavia nei diversi casi trattati profili comuni, che di seguito si evidenziano, segnalando altresì che a partire dall'aprile del 2011 la materia è stata affidata a un'unica unità organizzativa e che intensa è stata, in questo settore, l'attività di natura ispettiva effettuata dall'Ufficio, direttamente o avvalendosi della Guardia di finanza.

Il tema del controllo a distanza dei lavoratori mediante l'impiego di tecnologie (vecchie e nuove), già regolato dall'art. 4, l. n. 20 maggio 1970, n. 300 (nonché dall'art. 171 del Codice), rappresenta quello di più frequente oggetto delle segnalazioni che, non di rado, vengono indirizzate anche ai competenti uffici periferici del Ministero del lavoro (par. 10.1.).

Ricorrenti sono le richieste di utilizzare dati biometrici –anche al fine di commisurare il tempo di lavoro– che l'Autorità continua a ritenere, di regola, eccedenti, come già risulta dalle indicazioni di ordine generale fornite in passato (cfr., in particolare, il punto 4 del provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. *web* n. 1364099]) nonché il punto 7 del provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. *web* n. 1417809] (par. 10.2.).

Ulteriori e delicati ambiti di intervento hanno riguardato l'utilizzo di questionari di personalità –mediante i quali sono trattati anche dati sensibili, inerenti a sfere intime del lavoratore– in sede di assunzione, come pure in pendenza del rapporto di lavoro, al fine di dare attuazione alla disciplina sulla sicurezza sul lavoro, con particolare riferimento all'identificazione del fenomeno dello stress lavoro-correlato (questi ultimi all'esame dell'Autorità) (par. 10.3.).

Oggetto di lamentela è costituito talvolta anche dalle più varie operazioni di trattamento di dati personali riferibili a lavoratori nell'ambito dell'esecuzione del rapporto di lavoro: i

profili presi in esame riguardano l'utilizzo di informazioni personali per finalità diverse rispetto a quelle che ne avevano in origine giustificato la raccolta, le modalità di consegna della documentazione indirizzata al singolo lavoratore (contenenti, ad esempio, contestazioni disciplinari, notizie di carattere valutativo o sanitario) o (più in generale) l'accessibilità ad informazioni inerenti il singolo lavoratore da parte di altri colleghi (ad esempio, in ragione della configurazione data al protocollo informatico interno, ovvero a causa delle modalità di comunicazione prescelte dal datore di lavoro) (par. 10.4.).

Diverse questioni, spesso connesse alla trasparenza dell'attività amministrativa, riguardano l'applicazione delle 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], nonché delle linee-guida del Garante in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul *web* del 2 marzo 2011 (pubblicate in G.U. 19 marzo 2011, n. 64 [doc. *web* n. 1793203]), delle quali si è riferito nella Relazione 2010, p. 54 e ss.) con riferimento al regime di conoscibilità di dati riferiti a pubblici dipendenti (par. 10.5.).

Viene talora riproposta la questione inerente le condizioni di liceità del trattamento in relazione all'istituzione di procedure di segnalazione interna (cd. *"whistleblowing"*), tematica già oggetto di segnalazione al Parlamento e al Governo ai sensi dell'art. 154, comma 1, lett. *f*), del Codice da parte dell'Autorità (cfr. segnalazione 10 dicembre 2009 [doc. *web* n. 1693019]), ed almeno in parte oggetto di considerazione nell'ambito del più ampio processo legislativo che interessa la materia della corruzione (A.C. 4434 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione").

Tra i profili all'attenzione dell'Autorità va infine annoverata la corretta individuazione, nel rispetto del principio di pertinenza e non eccedenza (e spesso di indispensabilità, venendo in gioco dati sensibili), delle informazioni suscettibili di formare oggetto di trattamento in vista del riconoscimento delle agevolazioni previste dalla l. n. 5 febbraio 1992, n. 104 (legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate).

10.1. CONTROLLI A DISTANZA

Passando ad un esame più ravvicinato dei provvedimenti del Garante, merita sottolineare che tra le tecniche di controllo a distanza di più frequente oggetto di segnalazione e verifica da parte dell'Autorità, la videosorveglianza –più volte contemplata, anche in relazione al rapporto di lavoro, nei provvedimenti generali in materia adottati dall'Autorità (cfr. punti 4.1. del provv. 8 aprile 2010 [doc. *web* n. 1712680], e del precedente provv. 29 aprile 2004 [doc. *web* n. 1003482])– rimane ancora la più ricorrente (verosimilmente, trattandosi di quella di più agevole riconoscibilità da parte dei lavoratori, salvi i casi di controlli effettuati clandestinamente, talvolta rilevati in sede di verifica).

10.1.1. La videosorveglianza

In quest'ambito, i provvedimenti di divieto del trattamento dell'Autorità, fondati sull'inosservanza dell'art. 4, l. n. 300/1970 (o delle garanzie dallo stesso previste, vale a dire, il preventivo accordo con le rappresentanze sindacali dei lavoratori rispetto all'installazione delle apparecchiature di controllo o l'autorizzazione del competente ufficio periferico del Ministero del lavoro) –con la conseguente trasmissione degli atti all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali eventualmente configurabili– hanno riguardato una casa di cura, nella quale anche l'area occupata dal sistema di rilevazione delle presenze formava oggetto di ripresa (provv. 10 novembre 2011 [doc. *web* n. 1859539]; così pure nel caso deciso con provv. 16 febbraio 2012 [doc. *web* n. 1892377]), un centro di riabilitazione, nel quale formavano oggetto di ripresa gli accessi e i corridoi al piano (provv. 17 novembre 2011 [doc. *web* n. 1859546]), una società, nella quale le riprese interessavano gli ingressi principali e di emergenza, i corridoi ai diversi piani, nonché le aree di accesso a talune zone degli uffici (provv. 17 novembre 2011 [doc. *web* n. 1859558]), un hotel (provv. 14 aprile 2011 [doc. *web* n. 1810223]) e alcuni enti pubblici (provv. 10 novembre 2011 [doc. *web* n. 1859569]; provv. 2 febbraio 2012 [doc. *web* n. 1884167]; provv. 9 febbraio 2012 [doc. *web* n. 1886999]; provv. 16 febbraio 2012 [doc. *web* n. 1892377]). Talvolta si è reso necessario prescrivere la designazione quale "incaricato del trattamento" del personale preposto all'utilizzo del sistema di videosorveglianza ovvero disporre la riduzione dei tempi di

conservazione delle immagini registrate (provv. 17 novembre 2011 [doc. *web* n. 1859558) o, ancora, l'integrazione dell'informativa fornita agli interessati (provv. 10 novembre 2011 [doc. *web* n. 1859539]).

10.1.2. La geolocalizzazione

Di crescente rilevanza è il fenomeno della geolocalizzazione, in particolare di veicoli, che (di regola) consente anche l'individuazione degli spostamenti dei lavoratori che ne fanno uso (e princìpi non diversi possono trovare applicazione in relazione ad altre strumentazioni che determinano il medesimo effetto).

La tematica, già in passato oggetto di interventi dell'Autorità (cfr. provv. 7 ottobre 2010 [doc. *web* n. 1763071]), è stata riproposta con alcune verifiche preliminari presentate ai sensi dell'art. 17 del Codice (provv.ti 7 luglio 2011 [doc. *web* nn. 1828354 e 1828371]), nelle quali particolare attenzione è stata riservata all'individuazione dei dati suscettibili di trattamento, conformemente al principio di pertinenza e non eccedenza, considerate le finalità in concreto perseguite. Sono state ritenute lecite finalità riconducibili ad esigenze organizzative e produttive dell'azienda: in tali ipotesi, possono essere trattati solo i dati idonei a rilevare, quando necessario, la posizione dei veicoli nonché le sole informazioni indispensabili alla compilazione del rapporto di guida e per la commisurazione dei costi da imputare alla clientela (quali la distanza percorsa e il relativo consumo di carburante). Date le finalità in concreto perseguite dal titolare del trattamento, non si è invece ritenuto pertinente il trattamento di informazioni suscettibili di determinare un controllo sulla condotta di guida del conducente (dati tecnici relativi ai giri del motore ed alla frenata). In caso di esternalizzazione delle attività finalizzate alla localizzazione dei veicoli, il Garante ha evidenziato che il fornitore del servizio deve assumere il ruolo di responsabile del trattamento. I dati utilizzati per la regolare tenuta del libro unico del lavoro (disciplinata dall'art. 6, d.m. 9 luglio 2008), tra i quali quelli relativi alle presenze, alle ferie, ai tempi di lavoro, ed altri previsti dalle vigenti disposizioni, possono essere conservati per cinque anni.

Data la diffusione del fenomeno, la materia ha formato oggetto di un provvedimento generale di bilanciamento di interessi, con il quale sono state altresì impartite alcune

prescrizioni ai titolari del trattamento consentendo di avvalersi con maggiore speditezza di sistemi di geolocalizzazione, nel rispetto delle garanzie previste dalla disciplina di settore (prima fra tutte, quelle dettate dallo Statuto dei lavoratori) (provv. 4 ottobre 2011 [doc. *web* n. 1850581]). In base al provvedimento, quindi, i datori di lavoro pubblici e privati possono trattare (senza che sia necessario il consenso dei singoli lavoratori) dati personali ricavati da sistemi di localizzazione per soddisfare esigenze organizzative e produttive, ovvero per la sicurezza sul lavoro nell'ambito della fornitura di servizi di trasporto a condizione che, oltre la normativa sulla protezione dei dati personali, sia rispettata la disciplina dettata dall'art. 4, l. n. 300/1970. Ai lavoratori sottoposti a localizzazione devono essere forniti, oltre che gli elementi informativi prescritti dall'art. 13 del Codice, ulteriori ragguagli circa la natura dei dati trattati e le caratteristiche del sistema, da cui risulti con inequivocabile chiarezza che il veicolo è sottoposto a localizzazione (anche secondo il modello semplificato allegato al cit. provvedimento).

La materia, anche alla luce delle segnalazioni pervenute, ha formato altresì oggetto di attività ispettive, parte delle quali hanno interessato il settore del trasporto pubblico locale, i cui esiti sono, allo stato, in fase di valutazione.

10.1.3. Internet e data elettronica

Il trattamento di dati personali nell'utilizzo dei servizi di comunicazione elettronica (internet, posta elettronica aziendale nonché sistemi di telefonia su protocollo IP) –già oggetto, in termini generali, del provv. 1° marzo 2007 "Linee-guida per posta elettronica e internet" [doc. *web* n. 1387522]– nonché l'applicazione dei provvedimenti concernenti il ruolo e le funzioni degli amministratori di sistema nella sicurezza dei trattamenti (provv.ti 27 novembre 2008 [doc. *web* n. 1577499] e 25 giugno 2009 [doc. *web* n. 1626595]), hanno formato oggetto di verifica presso una società di primaria rilevanza. All'esito degli accertamenti, l'Autorità ha (tra l'altro) vietato la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione in internet dei dipendenti (tra i quali i tentativi di accesso di ogni singolo dipendente ai domini selezionati, con registrazione dei log indicanti tra l'altro la macchina utilizzata per l'accesso ad internet, indirizzo (*URL*) di

destinazione e utente richiedente), ritenendola in violazione degli artt. 11, comma 1, lett. *a*), c) e d), 113 e 114 del Codice nonché 4 e 8, l. n. 300/1970. Il *software* a tal fine utilizzato categorizzava le pagine filtrate ricorrendo ad una molteplicità di classi di siti visitati nonché la navigazione di ciascun utente secondo categorie predefinite dal sistema medesimo (quali, ad esempio, quelle denominate *adult material, advocacy groups, business and economy, entertainment, abortion, drugs, militancy and extremist*). La società disponeva di dati relativi alla navigazione internet riconducibili ad ogni singolo utente, conservati per un minimo di sei mesi, sino ad un anno, essendo vincolata alla disponibilità di spazio per l'archiviazione.

Inoltre, con riguardo al trattamento di dati personali effettuato dagli amministratori di sistema, è stato prescritto alla società di dare integrale attuazione alla prescrizione di cui alle lett. *c)* ed *f)* del citato provvedimento del 27 novembre 2008, assicurando in particolare che sia resa nota o conoscibile l'identità degli amministratori di sistema nell'ambito della società, nonché la completezza del tracciamento delle attività effettuate dagli amministratori di sistema. Il provvedimento adottato dal Garante nei confronti della società è stato impugnato davanti al Tribunale di Roma, che né ha sospeso gli effetti nelle more dello svolgimento del giudizio (provv. 21 luglio 2011 [doc. *web* n. 1829641]).

L'Autorità si è poi occupata di un reclamo che lamentava presunti illeciti controlli sul computer aziendale in uso all'interessata (provv. 7 aprile 2011 [doc. *web* n. 1812154]).

Dall'istruttoria è emerso che la società aveva illecitamente trattato i dati personali dell'interessata, ricavati da file di *backup* nell'ambito delle ordinarie operazioni di gestione del *server* aziendale. In particolare, non è risultato provato che la società avesse fornito all'istante un'idonea informativa preventiva relativamente ai trattamenti connessi all'utilizzo degli strumenti elettronici e ai correlati eventuali controlli, né che il trattamento fosse proporzionato rispetto alla finalità perseguita. L'Autorità ha quindi vietato alla società l'ulteriore trattamento dei dati personali dell'interessata ritratti dai file e documenti acquisiti in occasione delle operazioni di *backup*, invitando altresì il titolare a disciplinare le modalità di utilizzo degli strumenti elettronici conformemente alle istruzioni dell'Autorità, in particolare alle linee-guida su posta elettronica e internet del 1° marzo 2007 [doc. *web* n. 1387522].

10.1.4. Monitoraggio delle conversazioni di un call center

Ha altresì formato oggetto di esame il controllo a distanza degli operatori di un *call center* appartenenti ad una compagnia telefonica, in relazione ad operazioni di monitoraggio –realizzato previa registrazione delle conversazioni effettuate dagli operatori con gli utenti– dei processi aziendali di gestione del customer care. Trattandosi di vicenda relativa a dati, oltre che dei lavoratori, degli utenti se ne riferisce con maggiore dettaglio in altra parte (par. 11.3.), richiamando qui solo l'esito favorevole della valutazione del Garante, in ragione, tra l'altro, degli accordi sindacali conclusi con le rsa/rsu e degli accorgimenti tecnici e procedurali adottati dal titolare del trattamento (provv. 9 febbraio 2011 [doc. *web* n. 1797032]).

10.2. DATI BIOMETRICI

Coerentemente ad un orientamento consolidato (e sintetizzato nelle linee-guida sopra menzionate in materia di lavoro pubblico e privato), nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha ritenuto lecito il trattamento di dati biometrici ricavati dalla lettura delle impronte digitali effettuato da una società che opera nel settore della sicurezza privata, finalizzato unicamente a consentire l'accesso di un numero ristretto di dipendenti –mediante il confronto tra il *template* rilevato dal lettore e quello sullo stesso memorizzato in fase di *enrollment* (cd. *"matching on device"*) e senza memorizzazione di alcun dato ulteriore (in linea con l'art. 3 del Codice)– a determinate aree dello stabile aziendale destinate alla conta di denaro e alla custodia di beni di rilevante valore (provv. 10 giugno 2011 [doc. *web* n. 1835792]).

In una diversa ipotesi, segnalata dal dipendente di una società operante nel campo delle traduzioni e di servizi di interpretariato, il sistema biometrico utilizzato, centralizzando in una banca dati i *template* ricavati dalle impronte dei dipendenti, non è stato ritenuto lecito, non essendo stata dimostrata l'esistenza di "aree sensibili" che potessero giustificarne l'utilizzo in ragione della natura delle attività svolte, né essendo stato provato che il trattamento fosse conforme ai princìpi di necessità e proporzionalità, atteso che la società risultava essersi già dotata di un sistema di allarme e non risultava l'effettiva inefficacia delle ulteriori misure di protezione prospettate dalla società stessa (quali il servizio di portineria o l'utilizzo di *badge*)

(provv. 10 marzo 2011 [doc. *web* n. 1807683]). Nello stesso ordine di idee, un comune che aveva comunicato l'intenzione di istituire un sistema di rilevazione di impronte digitali per verificare la presenza dei dipendenti sul luogo di lavoro è stato invitato a verificare anche sulla base di quanto previsto al riguardo nelle citate linee-guida sul trattamento dei dati dei lavoratori in ambito pubblico (provv. 14 giugno 2007 [doc. *web* n. 1417809]) l'effettiva sussistenza delle particolari esigenze di controllo che consentono l'installazione di tali sistemi (nota 5 luglio 2011).

La tematica del trattamento di dati biometrici nel rapporto di lavoro è stata esaminata anche in sede di interpello preventivo (art. 17 del Codice). Con un primo provvedimento, adottato a seguito di un accertamento ispettivo espletato dal Ministero del lavoro, della salute e delle politiche sociali presso una società operante nel campo dell'edilizia per conto terzi, il Garante ha vietato l'ulteriore trattamento dei dati biometrici dei dipendenti effettuato allo scopo di rilevare la loro presenza sul posto di lavoro (provv. 20 ottobre 2011 [doc. *web* n. 1851657]). Ciò in quanto la società non aveva dimostrato l'effettiva sussistenza di eventuali aree "sensibili" (peraltro "esclusa" già in sede di accertamento ispettivo), né comprovato l'effettiva indispensabilità del trattamento alla luce delle finalità perseguite. Inoltre, non è risultato acquisito il libero consenso degli interessati, né che la società avesse fornito un'idonea informativa preventiva ai dipendenti relativamente al trattamento in esame.

L'Autorità si è inoltre riservata di valutare l'applicabilità di sanzioni.

Sempre in sede di interpello preventivo il Garante ha invece autorizzato, ritenendolo proporzionato alle finalità perseguite, il trattamento dei dati biometrici di alcuni dipendenti da parte di una società di ricerca, sviluppo e produzione di sistemi elettronici, anche per scopi militari (provv. 26 maggio 2011 [doc. *web* n. 1832558]).

Infatti il trattamento risultava preordinato a garantire l'accesso da parte del solo personale debitamente autorizzato a due sale *server* ubicate presso uno stabilimento adibito alla progettazione e alla realizzazione di sistemi di navigazione utilizzati a bordo di aerei militari e "contenenti apparati con applicazioni critiche e/o informazioni riservate" (astrattamente riconducibili a quelle "classificate" di cui alla l. n. 3 agosto 2007, n. 124 e al d.P.C.m. 3 febbraio 2006). L'adozione di adeguate misure di sicurezza "materiale" rispondeva a

specifiche esigenze previste a livello normativo e risultava funzionale a garantire l'osservanza degli stringenti requisiti di affidabilità richiesti dalle disposizioni ISO. Risultava conforme alla disciplina del Codice la prevista acquisizione del consenso libero ed espresso degli interessati (artt. 13 e 23 del Codice), come pure la predisposizione di adeguate misure di sicurezza (art. 31 e ss. e Allegato B. del Codice) relative anche alle modalità di accesso ai dati da parte degli amministratori di sistema e alla "tracciabilità" dei loro interventi.

L'Autorità ha tuttavia prescritto alla società, in luogo delle prospettate modalità centralizzate di conservazione dei *template* (ossia delle mappe delle impronte, codificate per impedire di risalire da esse alle immagini da cui sono tratte), di memorizzare questi ultimi su dispositivi posti nella esclusiva disponibilità degli interessati, per prevenire il rischio di eventuali utilizzi impropri delle informazioni o di possibili abusi. Alla società, inoltre, è stato prescritto di: impartire adeguate istruzioni circa l'eventuale perdita e sottrazione dei dispositivi affidati ai lavoratori; provvedere alla formale designazione degli incaricati e degli eventuali responsabili del trattamento; notificare al Garante il trattamento medesimo; rendere agli interessati un'idonea informativa preventiva; farsi rilasciare dall'installatore del sistema il prescritto attestato di conformità (regola n. 25 dell'Allegato B. del Codice).

10.3. QUESTIONARI DI PERSONALITÀ

Con provvedimento del 21 luglio 2011 [doc. *web* n. 1825852], impugnato in sede giurisdizionale, il Garante si è espresso in relazione a una procedura di selezione di un dirigente tecnico da parte di un ente pubblico economico, nella quale ai candidati erano stati somministrati, a cura di una psicologa, *test* di personalità contenenti dettagliate domande relative, fra l'altro, alla sfera affettiva, alla vita sessuale, alle condizioni di salute psico-fisica (con richiesta di indicare la patologia e il medicinale assunto, nonché le visite di natura psicologica/psichiatrica eventualmente effettuate); venivano inoltre richieste informazioni concernenti i disturbi del sonno, abitudini personali relative al fumo, al consumo di alcolici o di droghe ovvero inerenti ad abitudini alimentari o a tentativi di suicidio (effettuati o presi in considerazione dal candidato) nonché informazioni concernenti eventuali provvedimenti giudiziari di condanna, nonché, per le donne, eventuali interruzioni di gravidanza. Ritenuta

la co-titolarità del trattamento dei dati personali connesso alla somministrazione dei *test* di personalità in capo all'ente pubblico che aveva commissionato la selezione, alla società incaricata della sua esecuzione nonché alla psicologa che aveva somministrato i *test*, l'Autorità ha dichiarato l'illiceità del trattamento effettuato, ritenuto in violazione del principio di liceità (data la raccolta di informazioni vietate ai sensi dell'art. 8, l. n. 300/1970) nonché di pertinenza e non eccedenza, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2, del Codice.

Come anticipato, l'utilizzo di questionari di personalità caratterizzantisi per l'elevato dettaglio e la natura sensibile dei dati rilevati, ha formato oggetto di accertamento da parte dell'Ufficio (e gli esiti sono allo stato in corso di valutazione) non solo in fase assuntiva, ma anche al fine di individuare, in talune categorie di dipendenti, condizioni di stress lavoro correlato: gli esiti di tali accertamenti sono in corso di valutazione.

10.4. TRATTAMENTI IMPROPRI DI DATI PERSONALI

Tra le decisioni relative all'utilizzo di dati personali nell'ambito della gestione del rapporto di lavoro, merita evidenziare la riconosciuta illiceità, per violazione dei princìpi di necessità, finalità e liceità, del trattamento effettuato da una Direzione didattica di dati sensibili concernenti le condizioni di salute della sorella della segnalante (nonché la loro successiva comunicazione). Tali informazioni, infatti, contenute in documentazione originariamente prodotta dalla segnalante nell'ambito di un procedimento mirante al riconoscimento alla stessa dei benefici previsti dalla l. n. 104/1992, erano state successivamente utilizzate dal titolare del trattamento nell'ambito del diverso procedimento volto al riconoscimento, sempre in capo alla segnalante, di un'infermità per causa di servizio (provv. 12 gennaio 2012 [doc. *web* n. 1872998]).

In un altro caso un dipendente lamentava di aver ricevuto, da parte di personale non incaricato del trattamento dei dati, una missiva, recante gli indirizzi di altri (numerosi) destinatari, con la quale veniva comunicata, in forma cumulativa, l'entità delle ferie non fruite da ciascun lavoratore negli anni precedenti, nonché le ore di permesso non godute e quelle da recuperare. Il Garante, oltre a ritenere illecita tale modalità comunicativa poiché

non rispettosa dei princìpi di necessità e di non eccedenza, nel richiamare le puntuali indicazioni già fornite in ordine al corretto trattamento dei dati dei lavoratori nell'ambito delle attività di gestione del rapporto di lavoro privato, ha ritenuto illecito il trattamento evidenziando altresì la necessità di preporre alla custodia dei dati medesimi personale specificamente incaricato del trattamento (provv. 2 marzo 2011 [doc. *web* n. 1802433]).

10.5. DIFFUSIONE E COMUNICAZIONE DI DATI DI PUBBLICI DIPENDENTI

Le menzionate linee-guida del 14 giugno 2007, e quelle riguardanti il 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]) sono state richiamate in relazione ad una segnalazione relativa all'avvenuta pubblicazione, sul sito istituzionale di un comune, di una determina dirigenziale contenente dati relativi allo stato di salute di una dipendente. A seguito dell'intervento del Garante il comune ha prontamente rimosso dal sito *web* i dati oggetto della segnalazione (nota 12 luglio 2011).

Anche in un altro caso, nel quale un dirigente aveva lamentato la pubblicazione, sul sito istituzionale del comune dove prestava servizio, di taluni dati relativi a contestazioni disciplinari a suo carico contenuti in ordinanze del sindaco risalenti ad alcuni anni prima, a seguito dell'intervento del Garante il comune ha rimosso le ordinanze stesse dal sito *web* (nota 5 dicembre 2011).

Inoltre, in relazione a due analoghe vicende si lamentava rispettivamente l'affissione nell'albo pretorio comunale nonché nella bacheca di un'azienda ospedaliera di due determinazioni contenenti dati sulla salute degli interessati. In entrambe le occasioni l'Ufficio ha evidenziato che, in presenza di disposizioni che prevedono la pubblicazione obbligatoria delle deliberazioni adottate, nel rispetto dell'obbligo di adeguata motivazione degli atti amministrativi, occorre selezionare i dati da diffondere –in particolare se idonei a rivelare lo stato di salute, la cui diffusione è vietata– alla luce dei princìpi di pertinenza, non eccedenza ed indispensabilità dei dati trattati nonché delle indicazioni fornite con le citate linee-guida del 14 giugno 2007, del 19 aprile 2007 e del 2 marzo 2011 [doc. *web* n. 1793203] (note 27 dicembre 2011 e 23 gennaio 2012).

In un altro caso, alcuni dipendenti avevano lamentato la pubblicazione, sul sito istituzionale del Ministero della giustizia, di provvedimenti relativi al loro inquadramento, comprensivi di allegati contenenti il nominativo, il luogo e la data di nascita e il codice fiscale, dati che risultavano rinvenibili anche tramite i comuni motori di ricerca.

Il Garante ha premesso che occorre verificare, rispetto alle finalità della pubblicazione, se le informazioni contenute nei documenti debbano essere rese conoscibili a tutti e quindi liberamente reperibili sul sito istituzionale, ovvero ai soli interessati o ai contro interessati in un procedimento amministrativo (v. linee-guida 14 giugno 2007 e 2 marzo 2011, già citate). Ha inoltre rilevato che il Ministero, negli stessi provvedimenti oggetto di riproduzione sul sito *web*, aveva correttamente individuato, quale modalità adeguata per rendere conoscibile agli interessati la specifica documentazione, la pubblicazione di tali atti nella sezione intranet del sito *web* dell'Amministrazione, accessibile soltanto al personale, preceduta da un apposito avviso. Visto che la pubblicazione nella parte liberamente accessibile del sito istituzionale aveva comportato una diffusione non necessaria e sproporzionata in rapporto alla finalità perseguita anche in base alla disciplina di settore, il Garante ha ritenuto illecito il trattamento dei dati, ne ha quindi vietato l'ulteriore diffusione. È stato inoltre prescritto al Ministero di utilizzare in futuro modalità appropriate e proporzionate alle specifiche esigenze perseguite con la pubblicazione sul sito istituzionale di dati personali dei dipendenti, nel rispetto delle indicazioni fornite dal Garante con le citate linee-guida del 2 marzo 2011 (provv. 27 aprile 2011 [doc. *web* n. 1832775]).

In una diversa vicenda, il dipendente di un'azienda ospedaliera aveva segnalato che la copia della cartella sanitaria e di rischio rilasciatagli, su sua richiesta, dall'ospedale, recava la sigla del dirigente medico della struttura presso la quale prestava servizio in luogo di quella del medico competente. A tal proposito l'Autorità ha evidenziato, richiamando anche le citate linee-guida del 14 giugno 2007, che il datore di lavoro non può accedere alle informazioni contenute nella cartella sanitaria e di rischio del lavoratore essendo tenuto alla salvaguardia del segreto professionale. Alle medesime cautele, confermate dalla nuova normativa in materia di salute e sicurezza nei luoghi di lavoro, è tenuto il medico competente che ha il dovere di gestire la documentazione sanitaria curando le opportune misure di

sicurezza, nel rispetto del segreto professionale (punto 3.2. delle citate linee-guida del 14 giugno 2007; artt. 25, comma 1, lett. *c*), *d*) ed *e*), 39, comma 4, 41, comma 8 e 42 d.lgs. 9 aprile 2008, n. 81; v. anche il parere del Garante del 31 marzo 2008 [doc. *web* n. 1504941]). Nel caso di specie il medico competente avrebbe dovuto salvaguardare la segretezza e la sicurezza delle informazioni contenute nella documentazione sanitaria in suo possesso, trasmettendone copia in busta chiusa al datore di lavoro in modo tale da consentire a quest'ultimo di consegnarla all'interessato che ne aveva fatto richiesta. A seguito dell'intervento del Garante, l'azienda ospedaliera ha chiarito di aver accertato che la copia della cartella sanitaria e di rischio da consegnare al dipendente non necessita di autenticazione ed ha fornito idonee assicurazioni in relazione al rispetto, per il futuro, della disciplina sulla protezione dei dati personali (nota 23 dicembre 2011).

Dati sanitari del personale militare

Si richiama qui, perché attiene al trattamento dei dati di dipendenti, anche il parere reso al Ministero della difesa (parere 16 febbraio 2011 [doc. *web* n. 1797055]) sullo schema di decreto concernente le modalità di caricamento dei dati sanitari di emergenza nella tessera personale di riconoscimento del personale militare, Carta multiservizi della difesa (CMD), il cui testo tiene conto degli approfondimenti e delle indicazioni rese dall'Ufficio del Garante nel corso di riunioni e contatti informali, avviati sin dal 2008 (cfr. Relazione 2008, p. 142; v. anche par. 1.2.3.).

Nel corso del 2010, su sollecitazione dello stesso Ministero erano stati avviati, inoltre, approfondimenti sulla prassi di comunicare all'autorità di pubblica sicurezza i nominativi dei militari affetti da patologie psico-neurologiche ai fini della revoca dell'autorizzazione di Polizia a detenere armi a titolo privato (v. Relazione 2010, p. 140) nonché con riferimento all'indicazione della diagnosi nei certificati medici attestanti lo stato di malattia dei militari. A seguito di tali approfondimenti e delle indicazioni rese dall'Ufficio del Garante ai competenti uffici del Ministero, alcune proposte di modifica della normativa –in particolare per quanto attiene all'indicazione della diagnosi nei certificati medici e all'introduzione del sistema del cd. "doppio certificato"– sono state sottoposte nel 2011 all'Autorità, che ha espresso parere ai sensi dell'art. 154, comma 4, del Codice (provv. 22 settembre 2011 [doc. *web* n. 1844183] v. par. 1.2.3.)

10.6. PREVIDENZA

Un ufficio periferico dell'Istituto nazionale della previdenza sociale ha investito l'Autorità, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, di una richiesta finalizzata alla comunicazione ad un'azienda ospedaliera universitaria di dati concernenti la sussistenza di eventuali posizioni previdenziali nel casellario dei lavoratori attivi relativi ad un gruppo di lavoratori identificato in un arco temporale predeterminato. Finalità della comunicazione richiesta era quella dell'azienda di procedere a verifiche a campione sui propri dipendenti correlate al divieto dello svolgimento di attività incompatibili con il rapporto di pubblico impiego, come previsto dagli artt. 60-64, d.P.R. n. 3/1957, dall'art. 53, d.lgs. n. 165/2001 e dall'art. 1, commi da 56 a 65, l. n. 662/1996.

Il Garante, impregiudicato l'esercizio da parte dell'azienda delle prerogative riconosciute dall'art. 22, l. n. 241/1990, non ha accolto l'istanza presentata, sia per l'assenza di un'espressa previsione normativa che in via diretta ammettesse detta comunicazione, sia per la presenza di una puntuale disciplina (art. 39, comma 28, l. n. 27 dicembre 1997, n. 449 "Misure per la stabilizzazione della finanza pubblica") che consente di acquisire i dati necessari all'accertamento di eventuali situazioni di incompatibilità mediante la Guardia di finanza (provv. 24 novembre 2011 [doc. *web* n. 1880524]).

Nel corso dell'anno l'Ufficio ha ricevuto alcune segnalazioni con le quali si lamentava che una direzione dell'Inps aveva inviato comunicazioni contenenti verbali di accertamento dell'invalidità civile a persone diverse dagli interessati. Facendo seguito alla richiesta di informazioni ed alle indicazioni del Garante, l'Inps ha chiarito che si era trattato di un errore materiale ed ha assicurato di aver richiamato il personale addetto al rispetto delle regole sul trattamento dei dati personali (nota 20 gennaio 2012).

11. LE ATTIVITÀ ECONOMICHE

11.1. SETTORE BANCARIO

Provvedimento in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

Si è conclusa nel 2010 l'attività ispettiva avviata dal Garante presso alcuni importanti istituti e gruppi bancari, sulla base di numerose segnalazioni, che lamentavano indebiti accessi da parte di dipendenti alle informazioni bancarie dei clienti.

A seguito di tale attività il Garante ha adottato specifici provvedimenti (v. Relazione 2009, pp. 152-154, e Relazione 2010, pp. 132-134) ed ha altresì individuato profili problematici di carattere generale sul cui approfondimento ha coinvolto l'Abi. Quest'ultima ha elaborato un documento, in forma aggregata e anonima, relativo ad una rilevazione cui hanno partecipato "340 tra banche e gruppi bancari, che fanno complessivamente riferimento a 441 banche operanti sul territorio italiano" e che ha permesso una più dettagliata conoscenza dei meccanismi del settore, per una migliore definizione dell'intervento dell'Autorità.

In questo quadro, in assenza di una normativa che obblighi le banche a tracciare tutte le operazioni, l'Autorità ha adottato in data 12 maggio 2011 un provvedimento "in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie", pubblicato in G.U. 3 giugno 2011, n. 127 [doc. *web* n. 1813953], nel quale è stata prescritta agli istituti bancari l'adozione di rigorose misure.

In particolare è stato disposto che ogni operazione di accesso ai dati dei clienti (che comporti movimentazione di denaro o sia di semplice consultazione), effettuata da qualunque figura all'interno della banca, dovrà essere tracciata e registrata in un apposito log, nel quale devono essere contenuti: il codice identificativo del dipendente; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; il codice del cliente ed il tipo di rapporto contrattuale "consultato" (numero del conto corrente, fido, mutuo, deposito titoli). Tale misura ha lo scopo di assicurare che la banca sappia sempre il soggetto che ha avuto accesso ad un determinato conto corrente o ha effettuato operazioni ed il momento in cui ciò è avvenuto. I file di log di tracciamento delle operazioni, comprese quelle di semplice consultazione, dovranno essere conservati per almeno 24 mesi. Le banche, inoltre, dovranno prevedere l'attivazione di *alert* che individuino comportamenti anomali o a rischio (es. consultazioni massive, accessi ripetuti su uno stesso nominativo).

Almeno una volta l'anno la gestione dei dati bancari dovrà essere oggetto di un'attività di controllo interno, per verificare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalla normativa vigente. Il controllo, adeguatamente documentato, dovrà essere eseguito da personale diverso da quello che ha accesso ai dati dei clienti. Inoltre, verifiche sulla legittimità e liceità degli accessi, sull'integrità dei dati e delle procedure informatiche dovranno essere effettuate anche a posteriori, sia a campione sia a seguito di segnalazione.

Alle banche è stato infine raccomandato, come misura opportuna, di comunicare al cliente eventuali accessi non autorizzati al proprio conto e di rendere note al Garante eventuali violazioni di particolare rilevanza (per quantità, qualità dei dati, numero dei clienti).

11.2. INFORMAZIONI COMMERCIALI

Parziale modifica del provvedimento Ancic sull'esonero dell'informativa

Con provvedimento del 15 dicembre 2011 [doc. *web* n. 1862497] su istanza dell'Ancic (Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito) sono state rese meno onerose per le società associate, le modalità per rendere l'informativa semplificata agli interessati, in occasione del trattamento dei loro dati per finalità di informazione commerciale, già stabilite nel provv. 14 maggio 2009 [doc. *web* n. 1616828] (cfr. Relazione 2009, pp. 158-159).

In particolare, è stata prevista la pubblicazione, nella versione cartacea di "Pagine Gialle Lavoro", di un testo di informativa identico a quella attualmente resa, inserendo invece, alla voce "Ancic" riportata nell'elenco alfabetico di "Pagine Bianche" un semplice rimando al testo pubblicato su "Pagine Gialle Lavoro".

Il Garante ha previsto altresì l'inserimento, sui siti *web* di "Pagine Gialle" e di "Pagine Bianche", di appositi *banner* che consentano l'immediata apertura del testo dell'informativa e la pubblicazione, in maniera permanente sul proprio sito *web*, da parte di ciascuna società di informazione commerciale aderente ad Ancic, dell'informativa prevista dall'art. 13 del Codice, da evidenziarsi adeguatamente in autonomi riquadri di immediata consultazione.

L'Autorità, infine, ha prescritto, quale misura opportuna, che Ancic continui a tenere costantemente aggiornato l'elenco delle società di informazione commerciale aderenti, allo stato già presente sul sito *web* dell'Associazione.

11.3. ALTRE ATTIVITÀ IMPRENDITORIALI

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

Nell'ambito del trattamento dei dati personali degli utenti e dei lavoratori di *call center*, l'Autorità si è attivata a seguito di una segnalazione, che aveva rappresentato possibili profili di violazione della disciplina di protezione dei dati in relazione a un sistema di registrazione delle telefonate "in entrata" che una società stava implementando presso i propri gestori del servizio di *customer satisfaction*. Il sistema, diretto a migliorare la qualità del servizio di assistenza alla clientela attraverso un'analisi delle attività di "gestione" dell'utente da parte degli stessi *call center* (anche in vista di un eventuale miglioramento dei processi formativi del relativo personale), avrebbe garantito il rispetto dei princìpi del Codice attraverso opportuni accorgimenti volti, in particolare, a circoscrivere il trattamento dei dati personali degli interessati (campionatura delle telefonate registrate; alterazione della voce degli interlocutori; eliminazione degli orari di registrazione e dei primi secondi di conversazione; ecc.). L'impiego del sistema sarebbe stato preceduto da un'apposita informativa ai lavoratori interessati, mentre alla clientela tale informativa sarebbe stata resa in forma semplificata in occasione del collegamento con l'operatore, con possibilità di ricevere un'informativa più dettagliata collegandosi al sito della società.

All'esito dell'istruttoria condotta, il Garante, pur riconoscendo come meritevoli le finalità perseguite dalla società, ha tuttavia rilevato che l'informativa predisposta per l'utenza in occasione del contatto telefonico non dava sufficientemente conto delle finalità del trattamento, né indicava come poter accedere ad un'informativa più dettagliata. L'Autorità ha quindi prescritto alla società di integrare in tal senso l'informativa sintetica.

Il Garante ha poi ricordato come il trattamento in esame potesse essere effettuato dalla società solo con il consenso espresso degli interessati o in presenza di uno dei presupposti alternativi previsti dall'art. 24 del Codice. Considerato che un eventuale diniego del consenso avrebbe vanificato le finalità migliorative perseguite dalla Società, il Garante è intervenuto con un provvedimento di bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice), ritenendo che in questo caso il legittimo interesse del titolare del trattamento in riferimento a proprie esigenze di natura organizzativa e produttiva non potesse essere

considerato minusvalente rispetto ai diritti e alle libertà fondamentali degli interessati (provv. 9 febbraio 2011 [doc. *web* n. 1797032], v. al riguardo anche il par. 10.1.4.).

In un altro caso, l'Autorità è stata chiamata a pronunciarsi a seguito della richiesta di esonero di informativa da parte di una società operante nel settore dell'energia per l'allestimento di un sistema informativo volto a fornire ai vertici aziendali un costante aggiornamento sulla normativa in materia di energia e ambiente, nonché indicazioni sui soggetti istituzionali impegnati nel settore, compresi gli *opinion leader* regionali esperti in materia. In particolare, la società aveva chiesto di essere esonerata dall'obbligo di rendere l'informativa, sia in relazione al trattamento dei dati personali presenti nei siti *web* di tredici regioni italiane, concernenti soltanto il ruolo professionale dei predetti soggetti istituzionali, sia riguardo alle informazioni contenute nelle "relazioni" redatte all'esito di eventuali interlocuzioni con essi intervenute, ai sensi dell'art. 13, comma 5, del Codice.

L'Autorità, con provvedimento del 31 marzo 2011 [doc. *web* n. 1810147] non ha formulato alcun rilievo sulla realizzazione della banca dati normativa interna, non potendosi configurare rispetto ad essa alcun trattamento di dati personali.

Il Garante ha poi valutato che gli obiettivi del progetto, a sostegno di specifici uffici interni di gestione delle relazioni istituzionali, non fossero, in via generale, incompatibili con la finalità di informazione e trasparenza sottesa alla divulgazione via internet dei dati da parte degli enti pubblici titolari dei siti *web*. Inoltre, ha ritenuto di escludere i dati contenuti nelle "relazioni" relative agli incontri con "i soggetti decisori", dall'applicazione dell'art. 13, commi 4 e 5, del Codice, trattandosi di informazioni acquisite direttamente presso gli interessati nell'ambito dell'ordinaria attività lavorativa, peraltro oggetto di limitata divulgazione all'interno della società (soltanto 12 posizioni) nel rispetto degli ordinari vincoli gerarchici.

Pertanto, l'Autorità, ravvisando una manifesta sproporzione tra i mezzi necessari per rendere l'informativa e il diritto tutelato (stante la vastità del numero dei soggetti che istituzionalmente si occupano –anche solo a livello regionale– di energia ed ambiente), ha esonerato dall'obbligo di rendere l'informativa individuale agli interessati, in relazione al trattamento dei soli dati concernenti gli attori istituzionali acquisiti dai suindicati siti *web*, prescrivendo alla società di porre in evidenza, nella sezione *"compliance"* del proprio sito *web*, le caratteristiche del sistema

informativo e di specificare le finalità del trattamento, i tipi di dati che verranno reperiti negli specifici siti *web* regionali e le categorie di soggetti che formeranno oggetto di ricognizione.

In relazione ad un'ipotesi di fusione per incorporazione, l'Autorità si è espressa in merito all'istanza di una primaria società editoriale, che ha chiesto, in via principale, di essere esonerata dall'obbligo di rendere l'informativa agli interessati (tra cui, in particolare, gli abbonati e gli utenti dei siti internet) ed in via subordinata, –considerato che i trattamenti di dati riguardavano la stessa società ed alcune società da essa interamente controllate– di poter rendere la predetta informativa con modalità semplificate. L'istanza era motivata dal fatto che l'informativa secondo le modalità ordinarie avrebbe comportato, per il numero elevatissimo di interessati (oltre dieci milioni di persone) l'impiego di mezzi manifestamente sproporzionati rispetto ai diritti tutelati.

Con riferimento a richieste simili, ovvero di esonero dall'obbligo di rendere l'informativa in casi di fusione per incorporazione in ambito bancario (cfr. provv.ti 11 dicembre 2008 [doc. *web* n. 1584328]; 19 dicembre 2008 [doc. *web* n. 1584272]; 8 aprile 2009 [doc. *web* n. 1609999]), il Garante aveva rilevato, come affermato anche in giurisprudenza (Cass. civ. S.u., 8 febbraio 2006, n. 2637), che *"per effetto della fusione per incorporazione la società incorporante assume i diritti e gli obblighi della società incorporata, proseguendo, in tutti i rapporti (attivi e passivi) della medesima (anche processuali) anteriori alla fusione (art. 2504-bis, comma 1, c.c.)"*, e che pertanto anche i dati personali relativi a detti rapporti sono destinati ad essere trattati senza soluzione di continuità dalla società incorporante, la quale diviene unico titolare del trattamento senza dover procedere ad una (nuova) raccolta di dati.

Analogamente, nel caso in esame, si è osservato che la società incorporante avrebbe continuato l'attività delle società incorporate, nonché "il trattamento dei dati precedentemente svolto dalle incorporate (...), secondo le stesse modalità e per le medesime finalità di cui alle informative fornite dalle società precedenti titolari".

Pertanto, con provvedimento del 1° dicembre 2011 [doc. *web* n. 1872641], in attuazione dei princìpi di "correttezza" (art. 11, comma 1, lett. *a*), del Codice), "semplificazione, armonizzazione ed efficacia" (art. 2, comma 2, del Codice), l'Autorità ha prescritto alle società coinvolte nella predetta operazione di fornire agli interessati (attraverso i propri siti

web) i necessari aggiornamenti rispetto all'informativa resa dalle società oggetto della fusione e, tra essi, in particolare, di esplicitare la nuova denominazione del titolare del trattamento e gli estremi identificativi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali.

Trattamento dati personali dei disabili per l'acquisto di un'autovettura

Su sollecitazione della Federazione italiana dei concessionari di auto (Federauto) l'Autorità, con il provvedimento del 16 febbraio 2011 [doc. *web* n. 1792975], si è pronunciata sul trattamento di dati personali effettuato in occasione dell'acquisto di veicoli per i soggetti disabili, in vista dell'eventuale concessione dei benefici fiscali di legge, stabilendo le modalità di attuazione dei princìpi di necessità, pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *d*), del Codice).

A tal fine, il Garante ha previsto che gli organi competenti ad accertare le patologie per le quali viene previsto il beneficio fiscale indichino nelle certificazioni i soli dati pertinenti, completi e non eccedenti rispetto alle finalità per le quali debbono essere successivamente trattati nel procedimento di valutazione, e che gli operatori economici del settore trattino soltanto i dati effettivamente necessari per la definizione della specifica procedura valutativa; in particolare le imprese devono raccogliere la sola documentazione richiesta dalla legge.

Il Garante ha poi prescritto che i concessionari rendano agli interessati un'informativa dettagliata, indicando espressamente che i dati personali forniti –anche sensibili– potranno essere comunicati ad officine autorizzate in vista degli eventuali adattamenti da apportare ai veicoli acquistati, provvedendo, in quest'ultimo caso, ad acquisire anche il relativo consenso.

È stato inoltre previsto che trascorsi dieci anni, i dati personali, compresi quelli sanitari, salvo altre esigenze di conservazione (ad es. per controversie giudiziarie pendenti), dovranno essere distrutti, cancellati o trasformati in forma anonima. Infine, considerata l'ampiezza e la delicatezza delle informazioni trattate, l'Autorità ha raccomandato ai concessionari, alle imprese e alle officine autorizzate di adottare adeguate misure di sicurezza.

11.4. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Nel corso dell'anno, il Garante si è pronunciato in relazione ad una serie di istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società del settore privato.

Un'azienda che produce componenti meccanici di elevata precisione (in particolare, sfere di acciaio aventi caratteristiche qualitative e geometriche valutabili nell'ordine di centesimi di micron), destinati ad essere impiegati in diversi settori industriali, aveva chiesto di poter conservare per ventiquattro mesi le immagini acquisite attraverso il sistema di videosorveglianza in uso.

Avendo subìto numerosi atti di sabotaggio da parte di ignoti dopo la conclusione delle normali fasi di ispezione e di collaudo del "prodotto finito", la società, dal 2003, previo accordo con le rappresentanze sindacali unitarie, si era dotata del sistema per preservare la produzione e la competitività aziendale, evitando, al contempo, danni d'immagine che si sarebbero potuti riverberare anche sui livelli occupazionali.

L'Autorità ha rilevato che i ripetuti atti illeciti subiti dalla società in numerosi casi erano stati accertati soltanto a distanza di notevole tempo dalla loro commissione, al termine di fisiologici periodi di stoccaggio delle componenti meccaniche o, addirittura, dopo la loro successiva commercializzazione.

Pertanto, il Garante, ritenendo che l'installazione del sistema di videosorveglianza e l'allungamento dei tempi di conservazione delle immagini trovassero giustificazione in esigenze di tutela del patrimonio aziendale e di prevenzione di possibili atti di sabotaggio forieri di notevoli danni per l'azienda (oltre che per l'incolumità dei fruitori dei sistemi prodotti), ha accolto la richiesta di allungamento dei tempi di conservazione delle immagini in quanto conforme ai princìpi di non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*), del Codice (provv. 7 luglio 2011 [doc. *web* n. 1836347]).

Sempre in sede di verifica preliminare l'Autorità ha accolto la richiesta di allungare a 90 giorni i tempi di conservazione delle immagini registrate dal sistema di videosorveglianza di una società produttrice di fotomaschere, strumenti fondamentali per la realizzazione di dispositivi elettronici a circuito integrato (componentistica elettronica, *chips*, *smart card*, ecc.).

La richiesta di autorizzazione era stata motivata con l'esigenza sia di migliorare il livello di tutela della proprietà aziendale, sia di acquisire la qualità di "fornitore" di una società committente straniera, "leader mondiale" nel settore della sicurezza e fornitore ufficiale di molti governi, soggetta agli specifici protocolli di sicurezza fissati dagli *standard* ISO15408

(*"Common Criteria"*) e ISO17799 (codice di buona pratica per la gestione della sicurezza dell'informazione), di cui essa richiedeva l'osservanza anche ai propri fornitori.

L'Autorità ha autorizzato la conservazione limitatamente alle immagini degli eventi relativi agli effettivi allarmi, tenendo conto non solo dell'ubicazione isolata del sito e del delicato settore produttivo in cui opera l'azienda, ma anche della specifica attenzione, posta anche a livello internazionale, all'osservanza di elevati *standard* di sicurezza nelle produzioni relative al settore elettronico ed informatico.

In proposito, l'Autorità ha ritenuto che alcuni specifici *standard* ISO (definiti dalla *International Organization for Standardization*, di cui è membro anche l'Ente nazionale italiano di unificazione-Uni), recanti "specificazioni tecniche" volte a garantire rigorosi livelli di sicurezza, seppur giuridicamente non vincolanti, comunque fissano stringenti parametri qualitativi in settori di rilevante interesse pubblico e, al contempo, tecnologicamente assai complessi. In tal senso si è rilevato che spesso sono le stesse autorità pubbliche a promuoverne l'osservanza o fare diretto riferimento ad essi in atti ufficiali, mentre in ambito privatistico, stante l'esistenza di una consolidata prassi al loro inserimento negli schemi contrattuali nazionali ed esteri, tali norme sono divenute un punto di riferimento ineludibile in occasione della fornitura di opere o della prestazione di servizi ad alto contenuto tecnologico (provv. 14 luglio 2011 [doc. *web* n. 1836335]).

L'Autorità ha poi esaminato l'istanza di una primaria società di spedizione di documenti e pacchi in tutto il mondo, in prevalenza per via aerea, di prolungare fino a 30 giorni i tempi di conservazione delle immagini registrate presso i magazzini situati in alcuni aeroporti italiani.

La richiesta è stata giustificata con l'esigenza sia di rafforzare la sicurezza del patrimonio aziendale e delle spedizioni, sia di mantenere uno *standard* di sicurezza elevato, richiesto dalle regole del sistema di certificazione volontaria sulla qualità e sicurezza dei servizi aerei gestito da *"Transported Asset Protection Association"* (*TAPA*), ritenuto un "parametro di riferimento per gli adempimenti finalizzati a garantire la sicurezza dei trasporti e delle merci".

L'Autorità, nel rilevare che la società è soggetta a stringenti norme poste da regolamenti comunitari e, in via amministrativa, dall'Ente nazionale per l'aviazione civile (Enac), ha autorizzato la conservazione delle immagini al solo fine di consentire l'accertamento, da parte

dell'autorità giudiziaria, di eventuali illeciti verificatisi in occasione delle spedizioni, considerando che essi sono solitamente rilevabili solo dopo l'arrivo a destinazione della merce, spesso trattenuta per vari giorni nei magazzini.

Circa le norme poste dalla *"Transported Asset Protection Association"* (*TAPA*), è stato ritenuto che esse, pur essendo giuridicamente non vincolanti, sono comunemente considerate nel settore come fondamentali per garantire al meglio la sicurezza delle merci trasportate e, conseguentemente, per ridurre le perdite sofferte dalla catena di approvvigionamento internazionale, prevenendo furti e danneggiamenti, legati, in alcuni casi, anche ad atti di terrorismo internazionale (provv. 10 novembre 2011 [doc. *web* n. 1877751]).

L'Autorità si è da ultimo pronunciata in merito all'istanza di una società concessionaria dell'Anas di poter conservare per venti giorni alcune immagini acquisite (con l'accordo delle rappresentanze sindacali) attraverso il sistema di videosorveglianza in uso presso le stazioni autostradali del tratto in concessione.

L'Autorità ha ritenuto tale periodo di conservazione giustificato in ragione sia della programmazione dei prelievi presso le stazioni autostradali (in alcuni casi, trascorrono anche dieci giorni dal momento del versamento del denaro da parte del personale di esazione o del cliente presso le casse self-service), sia soprattutto dei tempi necessari ad altra società che, per conto della concessionaria di Anas, una volta prelevato l'incasso, effettua il servizio di conteggio e rendicontazione del denaro, anche in vista dell'espletamento di indagini giudiziarie che dovessero rendersi necessarie in caso di illeciti accertati dopo le 24 ore dall'esazione dei pedaggi (art. 11, comma 1, lett. *d*) ed *e*), del Codice) (provv. 17 novembre 2011 [doc. *web* n. 1877929]).

Di altri provvedimenti relativi alla videosorveglianza si da conto nel paragrafo 10.1.1.

12. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Particolarmente intensa nel 2011 è stata l'attività del Garante nel settore dei trasferimenti transfrontalieri di dati personali attraverso il rilascio sia di autorizzazioni ad hoc in materia di *Binding Corporate Rules - BCR* (norme vincolanti di impresa), sia di autorizzazioni di carattere generale, volte ad attuare alcune decisioni della Commissione europea in merito all'adeguatezza della normativa di protezione dei dati offerta da un Paese non appartenente all'Unione europea (decisione di cui all'art. 25, paragrafi 1 e 2, della Direttiva n. 95/46/CE).

Con riferimento alle *BCR*, l'Autorità, con i provvedimenti del 5 maggio 2011 [doc. *web* n. 1829762] e dell'11 ottobre 2011 [doc. *web* n. 1849957], si è pronunciata in ordine allo schema di norme vincolanti d'impresa elaborato da un'importante gruppo societario di carattere multinazionale operante nel settore della produzione di pneumatici.

Al Garante sono pervenute due istanze di autorizzazione al trasferimento di dati personali verso Paesi terzi relative al medesimo progetto di *BCR*, approvato a seguito della conclusione di una procedura di cooperazione europea coordinata dalla *Commission nationale de l'informatique et des libertés* (Autorità francese in materia di protezione dei dati) ai sensi del sistema di mutuo riconoscimento, volto a semplificare l'esame degli schemi predisposti dalle società (v. Relazione 2009, p. 189).

La prima richiesta di autorizzazione è stata presentata da una società per azioni, filiale italiana del gruppo multinazionale sopra indicato, con riferimento ai trasferimenti verso le altre filiali del gruppo con sede in Paesi non appartenenti all'Unione europea. L'istanza aveva ad oggetto i trasferimenti dei dati personali relativi: ai dipendenti e ai candidati all'assunzione, per finalità connesse rispettivamente alla gestione del rapporto di lavoro e del processo di selezione; ai fornitori e ai clienti, per finalità amministrativo contabili inerenti al rapporto contrattuale; ai consumatori, per rispondere a richieste di informazioni o a reclami; ai giornalisti, per la trasmissione di comunicati stampa o di inviti ad eventi promozionali.

Il Garante, a seguito di una complessa istruttoria, nel corso della quale ha preso atto delle dichiarazioni integrative rese dalla richiedente Autorità (relative, in particolare, all'efficacia vincolante dell'accordo intra-gruppo con cui le filiali si impegnano al rispetto delle norme

vincolanti d'impresa, all'esatta indicazione dei dati trasferiti e delle finalità dei trasferimenti e all'obbligo di rilascio di idonea informativa agli interessati), ha autorizzato il trasferimento summenzionato secondo le modalità fissate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate. Il Garante ha comunque ribadito il proprio potere di svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, eventuali provvedimenti di blocco o di divieto. Infine, ha precisato che le operazioni di trattamento dei dati personali, anche se poste in essere a seguito del rilascio dell'autorizzazione, sono lecite solo ove conformi alla normativa nazionale vigente e alle sue successive modificazioni, anche in materia di protezione dei dati personali, con particolare riferimento alle specifiche disposizioni sui presupposti di legittimità delle attività di raccolta dei dati oggetto del trasferimento e sulla sussistenza dei presupposti di legittimità per la comunicazione dei dati medesimi.

Nel secondo caso, l'istanza di autorizzazione è stata presentata da una fondazione, stabilita in Italia e appartenente al medesimo gruppo multinazionale d'impresa, al fine di ottenere l'autorizzazione del Garante ai trasferimenti infragruppo tramite *BCR* verso altre filiali stabilite in Paesi terzi e relativamente ai soli dati personali dei clienti trasferiti, per finalità amministrativo contabili inerenti al rapporto contrattuale.

Anche in questa ipotesi, il Garante ha effettuato una complessa istruttoria, chiedendo opportuni chiarimenti in merito all'individuazione dei soggetti coinvolti nel trasferimento transfrontaliero dei dati personali e all'effettiva conclusione, da parte della fondazione summenzionata, dell'accordo infragruppo con cui si garantisce efficacia vincolante alle *BCR*.

L'autorizzazione è stata rilasciata nei limiti delle modalità di trasferimento indicate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate.

In termini più generali nel 2011 si è notevolmente ampliato il numero dei Paesi non appartenenti all'Unione europea considerati adeguati ai sensi dell'art. 25, paragrafi 1 e 2 della Direttiva n. 95/46/CE, per il livello di protezione dei dati personali da essi fornito.

Questa Autorità ha, infatti, recepito con proprie autorizzazioni generali le decisioni della Commissione europea in merito all'adeguatezza delle normative di protezione dei dati

personali del Principato di Andorra (autorizzazione 3 febbraio 2011 [doc. *web* n. 1788981]; delle Isole Fær Øer (autorizzazione 7 settembre 2011 [doc. *web* n. 1838283]); del Baliato di Jersey (autorizzazione 7 settembre 2011 [doc. *web* n. 1838359]) e dello Stato di Israele (autorizzazione 20 gennaio 2012 [doc. *web* n. 1868817]).

In questo modo si consente ai titolari stabiliti nel territorio dello Stato italiano di trasferire dati personali verso uno dei Paesi oggetto dell'autorizzazione senza l'adempimento di ulteriori formalità (quali ad es. clausole contrattuali tipo, *BCR*, autorizzazioni *ad hoc*).

Nell'autorizzare tali trasferimenti, l'Autorità si è riservata di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento.

Trasferimento di dati personali in Argentina

Il Ministero degli affari esteri ha richiesto la collaborazione del Garante per dare attuazione al *Memorandum* di intesa fra l'Italia e l'Argentina firmato il 1° giugno 2011 ai fini del trasferimento alle autorità argentine di documentazioni d'archivio, custodite presso la rete diplomatico-consolare italiana in Argentina, concernenti le vittime della dittatura militare (1976-1983). Tale collaborazione è avvenuta nell'ambito dei lavori della commissione tecnica bilaterale appositamente istituita, nel corso dei quali le autorità argentine hanno dichiarato che le finalità della richiesta della documentazione riguardavano la ricostruzione del periodo storico degli anni della dittatura. In particolare, in tale occasione è stato stabilito che copia ufficiale della documentazione custodita negli archivi consolari relativa a cittadini italiani, doppi cittadini o cittadini di origine italiana, vittime del regime militare argentino, sarebbe stata consegnata all'Archivio nazionale della memoria che l'avrebbe utilizzata esclusivamente per i propri fini istituzionali, stabiliti con il decreto della Repubblica Argentina, n. 1259/2003, in conformità alla vigente normativa argentina sulla protezione dei dati personali, nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate.

In seguito, il Ministero degli affari esteri, nell'illustrare formalmente al Garante il contenuto dei lavori della commissione, attesa l'impossibilità di comunicare singolarmente agli interessati l'imminente trasferimento della predetta documentazione, ha rappresentato l'intenzione di informare adeguatamente e tempestivamente gli interessati in Italia e presso la

collettività argentina attraverso un'apposita informativa (di cui ha fornito copia), da pubblicare nei due mesi antecedenti alla prima consegna del materiale e nei quattro mesi successivi sul proprio sito istituzionale, nonché su quelli dell'Ambasciata d'Italia a Buenos Aires e dei Consolati dipendenti, e da divulgare attraverso i canali consolari. Il Ministero degli affari esteri ha, inoltre, precisato che la consegna della copia della documentazione all'Archivio della memoria avverrà gradualmente, in plico chiuso sigillato, dopo aver espletato, ove necessario, le procedure previste dalla normativa in vigore in materia di utilizzo di documentazione classificata.

Con il provvedimento del 25 gennaio 2012 [doc. *web* n. 1872111], il Garante, sulla base della propria autorizzazione del 9 giugno 2005, relativa al trasferimento dei dati personali verso l'Argentina (adottata in conformità alla decisione della Commissione europea del 30 giugno 2003, n. 2003/490/CE, con la quale è stato considerato adeguato il livello di protezione dei dati personali offerto dalle disposizioni di rango costituzionale e dalle altre norme vigenti in Argentina), ha ritenuto che il trasferimento dei dati personali contenuti nella documentazione in parola non fosse contrastante con il Codice e che le garanzie individuate dal Ministero degli affari esteri e dalla commissione tecnica bilaterale fossero idonee ad assicurare il rispetto dei diritti degli interessati.

13. LIBERE PROFESSIONI

13.1. ATTIVITÀ FORENSE E INVESTIGATIVA

Nel corso del 2011 sono pervenute all'Autorità alcune segnalazioni relative al trattamento di dati personali nell'ambito dell'attività forense e investigativa.

Trattamento dati per fare valere un diritto in sede giudiziaria

Con una segnalazione è stato lamentato che un avvocato aveva allegato un provvedimento giudiziale contenente dati personali del segnalante alla richiesta rivolta all'anagrafe di un comune di verificare la residenza dell'interessato stesso.

Il Garante ha rilevato che il trattamento dei dati del segnalante è stato effettuato *"per far valere o difendere un diritto in sede giudiziaria"*, finalità che ricorre anche quando i dati sono trattati nel corso di un procedimento amministrativo (quale l'accertamento della residenza da parte dell'anagrafe comunale) e nella fase propedeutica all'instaurazione di un eventuale giudizio. In relazione a tale finalità, l'informativa all'interessato e il suo consenso non sono richiesti (artt. 13, comma 5, lett. *b*), e 24, comma 1, lett. *f*), del Codice) ed anche i dati sensibili possono essere trattati senza consenso, previa autorizzazione del Garante (art. 26, comma 4, lett. *c*), del Codice; v. autorizzazione n. 4/2011 al trattamento dei dati sensibili da parte dei liberi professionisti del 24 giugno 2011 [doc. *web* n. 1822597]).

Alla luce delle disposizioni citate, il trattamento dei dati effettuato dall'avvocato è risultato, pertanto, lecito (nota 26 ottobre 2011).

L'Autorità si è espressa nello stesso senso in un caso in cui il trattamento dei dati personali del segnalante era avvenuto tramite una e-mail spedita dall'avvocato della controparte precedentemente all'avvio di un contenzioso in sede giudiziaria (nota 27 dicembre 2011).

Attività investigative

In risposta ad un quesito presentato da un investigatore privato, concernente la legittimità della raccolta di dati personali nell'ambito di un'attività finalizzata all'accertamento di eventuali frodi assicurative, il Garante ha evidenziato che per far valere o difendere un diritto in sede giudiziaria l'investigatore risulta legittimato a presentare la richiesta di accesso ai dati, con esonero dagli adempimenti dell'informativa e del consenso, sempre che i dati siano trattati esclusivamente per la finalità citata e per il periodo strettamente necessario al suo perseguimento (cfr. art. 9 del codice di deontologia e di buona condotta per i trattamenti di

dati personali effettuati per svolgere investigazioni difensive (Allegato A.6. al Codice). L'Autorità ha inoltre precisato che in tali ipotesi il trattamento di dati sensibili deve conformarsi alle disposizioni contenute nell'autorizzazione n. 6/2011 al trattamento dei dati sensibili da parte degli investigatori privati [doc. *web* n. 1822629] e, se necessario, a quelle di cui all'autorizzazione n. 2/2011 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale [doc. *web* n. 1822577].

Il Garante ha, infine, precisato che la normativa richiamata autorizza, alle condizioni ivi contenute, l'investigatore al trattamento dei dati dell'interessato, ma non prevede il diritto di ottenere le informazioni né l'obbligo per i soggetti pubblici o privati che li detengono a consegnarli a persona diversa dall'interessato medesimo (nota 8 agosto 2011).

Produzione di documenti in giudizio

Con riferimento specifico alla produzione documentale in sede giudiziaria, il Garante, richiamando il proprio orientamento in materia (provv. 23 settembre 2010 [doc. *web* n. 1756065]; provv. 4 novembre 2010 [doc. *web* n. 1770943]; provv. 17 novembre 2010 [doc. *web* n. 1779765]), ha confermato che spetta al giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali. Infatti, l'art. 160, comma 6, del Codice stabilisce che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (si citano, a titolo esemplificativo, le note 25 gennaio, 15 febbraio, 1° marzo, 13 luglio, 3 novembre 2011).

Comunicazione di dati presso il luogo di lavoro

È stato sottoposto all'attenzione del Garante l'invio, da parte dell'avvocato dell'*ex* moglie del segnalante, di una diffida stragiudiziale indirizzata nel luogo di lavoro del segnalante stesso.

Dall'istruttoria è risultato, in particolare, che la diffida era stata inviata direttamente al segnalante presso il suo luogo di lavoro, che rientra, peraltro, tra i luoghi ove può essere eseguita la notificazione degli atti del processo civile, ai sensi dell'art. 139 c.p.c..

Il trattamento dei dati effettuato dall'avvocato è risultato, pertanto, lecito (nota 28 settembre 2011).

Diversa la soluzione nel caso di un avvocato che aveva inviato al datore di lavoro del suo cliente una lettera raccomandata di sollecito nella quale, in pretesa applicazione dell'art. 139

c.p.c. –che disciplina la notifica di atti all'interessato presso la sua casa di abitazione o dove ha l'ufficio o esercita l'industria o il commercio– aveva ingiunto al cliente di pagare la parcella, avvertendo che, in difetto, avrebbe avviato la procedura esecutiva procedendo, se del caso, anche nei confronti del datore di lavoro.

Il Garante ha ritenuto che il trattamento non poteva trovare giustificazione nell'art. 139 c.p.c., poiché la comunicazione dei dati personali del cliente era stata effettuata non al medesimo presso il suo luogo di lavoro, bensì a persona diversa, ossia direttamente al suo datore di lavoro.

L'Autorità ha pertanto ritenuto il trattamento dei dati personali in contrasto con le disposizioni del Codice, secondo le quali tali dati debbono essere trattati in modo lecito e secondo correttezza (art. 11), l'interessato deve essere previamente informato del trattamento dei propri dati personali (art. 13) ed il trattamento di essi da parte dei privati è ammesso solo con il consenso espresso dell'interessato stesso (art. 23) (nota 4 marzo 2011).

14. Il Registro dei trattamenti

Rientra tra i compiti dell'Autorità tenere il registro dei trattamenti, formato sulla base delle notificazioni ricevute, e renderlo accessibile a chiunque, nonché determinare le modalità per la sua consultazione gratuita per via telematica (art. 154, comma 1, e art. 37, comma 4, del Codice).

L'Autorità ha garantito tali condizioni di accessibilità già dall'attivazione del Registro nel 2004, curando la realizzazione di una procedura di notificazione telematica e dedicando alla consultazione *online* del registro un'apposita sezione del suo sito internet.

Il titolare di un trattamento di dati personali, nei casi e nei modi previsti dagli artt. 37 e 38 del Codice, è obbligato a comunicare il trattamento stesso al Garante, salve le ipotesi di esonero (v. Relazione 2004, p. 109, provv. 31 marzo 2004 [doc. *web* n. 852561]; nota 23 aprile 2004 [doc. *web* n. 993385]; nota 26 aprile 2004 [doc. *web* n. 996680]; provv. 24 giugno 2011 [doc. *web* n. 1823225]). Tale comunicazione avviene attraverso la notificazione, che consiste in una dichiarazione formale compilata direttamente sul computer dell'utente, per il tramite di un'apposita procedura disponibile sul sito dell'Autorità, che è stata semplificata riguardo, in particolare, alle modalità di compilazione del modello informatico e ai suoi contenuti (provv. 22 ottobre 2008 [doc. *web* n. 1571196]).

In tale quadro, nel 2011 il Garante ha esonerato dall'obbligo di notificazione, il trattamento di dati genetici da parte degli organismi di mediazione nell'ambito dell'attività finalizzata alla conciliazione delle controversie civili e commerciali (provv. 24 giugno 2011 [doc. *web* n. 1823225]). L'Autorità ha, infatti, ritenuto che i trattamenti di dati genetici da parte di questi organismi (la cui attività è prevista dal d.lgs. 4 marzo 2010, n. 28 e successive modificazioni e integrazioni e regolamentata dal d.m. 18 ottobre 2010, n. 180) presentassero carattere saltuario e non prevalente nell'ambito di quelli complessivamente effettuati.

L'assistenza operativa ed il supporto tecnico ed amministrativo nei confronti dei titolari dei trattamenti sono da sempre garantiti da diverse tipologie di servizio. In primo luogo da quello di messaggistica automatica originato dalla procedura telematica di notificazione. Secondariamente dal servizio di posta elettronica gestito direttamente dal personale addetto, ora anche nella forma della PEC, infine attraverso il supporto telefonico.

Complessivamente tali strumenti consentono di rispondere pienamente alle diverse esigenze dell'utenza.

Si mantengono costanti gli accessi diretti al Registro da parte degli utenti, con una media giornaliera vicina ai 90 accessi e punte superiori ai 300. È consentita agli utenti la stampa integrale delle notificazioni.

È continuata nel 2011 la tendenza alla ripresa, +2% circa, del numero di notificazioni presentate, con un sostanziale riallineamento al dato del 2008.

I dati percentuali relativi alla tipologia dei trattamenti notificati nel 2011 non si discostano da quelli del periodo 2004-2010. I trattamenti volti a definire il profilo e la personalità dell'interessato tramite l'ausilio di strumenti elettronici (27%), di dati idonei a rivelare lo stato di salute e la vita sessuale (22%) e quelli relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (19%, peraltro in flessione di un punto percentuale rispetto al 2010), coprono da soli quasi il 70% di tutti i trattamenti notificati.

È opportuno segnalare solo un lieve aumento –dall'8% al 9%– dei trattamenti che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica.

In merito infine alla distribuzione geografica dei titolari, vale quanto già evidenziato negli anni precedenti. Il nord del Paese esprime da solo il 57% dei notificanti. Tale decisa prevalenza potrebbe essere ascrivibile tanto a diversità economiche di natura strutturale quanto ad una più decisa incidenza della crisi economica sulla tipologia dei titolari con sede nel meridione (ditte individuali, artigiani, società a responsabilità limitata di piccole o piccolissime dimensioni).

Va rilevato poi, che nel 2011 le notificazioni presentate direttamente dai titolari hanno superato in numero assoluto quelle presentate tramite intermediario. Tale novità è da attribuirsi al sempre più diffuso utilizzo della firma digitale e, più in generale alla maggiore confidenza con le procedure telematiche nei rapporti con le pubbliche amministrazioni.

Si segnala, infine, che la disciplina della materia potrebbe costituire oggetto di modifiche, nell'ambito della proposta, presentata dalla Commissione europea il 25 gennaio 2012, di un

regolamento generale sulla protezione dei dati personali destinato a sostituire la Direttiva n. 95/46/CE. Nel testo si ipotizza l'abolizione dell'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito da quello di nominare un *"data protection officer"* (incaricato della protezione dati, secondo la terminologia della Direttiva n. 95/46) per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti.

15. LA TRATTAZIONE DEI RICORSI

Come nelle precedenti relazioni, in questo capitolo si svolgono, in ragione dell'ampiezza e della trasversalità delle questioni oggetto dei ricorsi presentati al Garante, riflessioni di carattere più generale, riguardanti anche materie trattate in altre parti di questa Relazione.

La prima riflessione che è possibile fare esaminando complessivamente i ricorsi istruiti e decisi dall'Autorità nell'anno 2011 è la constatazione della sensibile diminuzione del numero dei casi sottoposti, nell'anno appena trascorso, all'attenzione del Garante. I 257 ricorsi decisi nell'anno 2011 segnano infatti un calo di cento unità circa rispetto all'anno precedente e rappresentano un totale molto lontano dalle cifre raggiunte nei primi anni dello scorso decennio. Il fenomeno è significativo e merita di essere esaminato, anche se l'interpretazione dello stesso appare complessa ed esposta al rischio di semplificazioni. Comunque è possibile proporre alcune riflessioni di massima, che permettono, più in generale, di valutare come la legge sulla protezione dei dati personali sia vissuta e percepita oggi.

15.1. LA PIÙ DIFFUSA CONOSCENZA DELLA LEGGE

Anzitutto va evidenziato come, a circa quindici anni dall'introduzione nell'ordinamento giuridico italiano della disciplina in materia di protezione dei dati personali, la consapevolezza delle nuove situazioni giuridiche soggettive è sicuramente penetrata in maniera significativa nel tessuto delle conoscenze degli operatori economici e del diritto. In altre parole, porsi il problema di accedere ai dati personali, di conoscerne l'origine, di opporsi al loro trattamento significa, ormai, attivare meccanismi di tutela percepiti come "ordinari" e "naturali", da utilizzare appropriatamente a seconda delle circostanze, magari per acquisire gli elementi conoscitivi di base sui quali impostare più complessi contenziosi. In questo senso (e talvolta con qualche inevitabile confusione) i diritti contemplati dall'art. 7 del Codice si possono paragonare a quelli attivabili ai sensi della legge n. 241/1990, in materia di accesso agli atti e ai documenti amministrativi, o a quelli contemplati, in altro ambito, dal codice del consumo, o dal testo unico bancario o dal codice delle assicurazioni private. Tutti testi normativi che si muovono nella prospettiva di favorire la trasparenza di significativi ambiti contrattuali o di estendere le possibilità conoscitive del cittadino utente, risparmiatore, ecc..

L'ampia conoscenza e il diffuso utilizzo degli strumenti di tutela previsti dal Codice ha sicuramente inciso sul contenzioso portato all'attenzione del Garante con lo strumento del ricorso *ex* artt. 145 ss.. Questo infatti è uno strumento di secondo livello, che si può attivare solo nel caso in cui il titolare del trattamento, destinatario di una richiesta ai sensi del citato art. 7, non abbia fornito adeguato riscontro all'interessato. È facile constatare come negli ultimi anni i titolari del trattamento (specie quando si tratta di enti pubblici o di grandi società di servizi) si siano strutturati dal punto di vista organizzativo in modo da corrispondere in modo tempestivo alle richieste degli interessati. Il ricorso, dunque, non è più, nella stragrande maggioranza dei casi, la denuncia di un atteggiamento totalmente omissivo da parte del soggetto chiamato a dare ragione del trattamento dei dati dell'interessato, ma si sostanzia nella contestazione nel merito di riscontri ritenuti volta a volta incompleti, elusivi o illegittimi.

In qualche modo si può semplificare il ragionamento affermando che molti ricorsi del passato (quando il dato quantitativo dei procedimenti attivati era molto significativo) erano lo specchio di una iniziale difficoltà di molti soggetti a corrispondere alle richieste degli interessati, mentre oggi, spesso, prevale il profilo qualitativo, indotto dalla esigenza di mettere a fuoco, nel merito, profili di protezione dei dati di particolare complessità.

15.2. AMBITI E ORIENTAMENTI CONSOLIDATI

Come è naturale, in una prima fase il contenzioso affrontato con lo strumento del ricorso ha interessato i più vari ambiti, ricercando tutti gli spazi possibili per ottenere una tutela rapida ed efficace dei diritti lesi.

In dodici anni di esperienza nell'ambito dei ricorsi si è così creata e sedimentata una "giurisprudenza" dell'Autorità che su determinati "filoni" costituisce ormai un punto di riferimento ineludibile, ben conosciuto da tutti i soggetti interessati e largamente asseverato dalle sentenze dei giudici aditi in sede di opposizione ai sensi dell'art. 152 del Codice. Ciò spiega perché alcuni temi che avevano dato luogo ad un ampio contenzioso e alla presentazione di molti ricorsi negli anni passati occupino ormai uno spazio ridotto nelle statistiche più recenti. Basti pensare, a questo riguardo, alle richieste di accesso ai dati personali di tipo valutativo, con particolare riguardo a quelli contenuti nelle perizie medico-

legali redatte in ambito assicurativo. Il tema, che aveva caratterizzato specialmente gli anni a cavallo dell'entrata in vigore del nuovo Codice, ha trovato ora, grazie anche al più esplicito riferimento contenuto nell'art. 8, comma 4, del Codice stesso, un suo assestamento, sia in relazione alle situazioni (largamente maggioritarie) nelle quali la richiesta di accesso a tali dati è rapidamente soddisfatta, sia in riferimento ai casi (invero pochi) nei quali tale accesso è differito in ragione della presenza di legittime esigenze difensive e di tutela delle ragioni del titolare del trattamento (art. 8, comma 2, lett. *e*), del Codice).

Rispetto ai primi anni dello scorso decennio è parimenti riscontrabile una sensibilissima diminuzione dei ricorsi proposti con riferimento al trattamento dei dati personali svolto presso le società che gestiscono sistemi di informazioni creditizie. In questo caso la spiegazione sta nell'efficace opera di "sistemazione" normativa del settore cui il Garante ha dato un prezioso e, di fatto, decisivo contributo, promuovendo e accompagnando fino alla conclusione i lavori di redazione del codice deontologico che, a far data dal 2005, disciplina questa amplissima categoria di dati.

15.3. ALTRE FORME DI TUTELA

Nell'esaminare le ragioni del progressivo calo del numero di ricorsi pervenuti negli ultimi anni non si può fare a meno di rilevare come a tale fenomeno si sia associato un parallelo aumento delle decisioni dell'Autorità a seguito della proposizione di reclami e segnalazioni.

Questo, in realtà, è il portato del dettato normativo del Codice, che negli artt. 141 e ss. ha delineato le caratteristiche di fondo degli strumenti di tutela attivabili di fronte all'Autorità, ma, soprattutto, è la conseguenza delle disposizioni attuative (regolamenti nn. 1 e 2/2007) che a far data dal 2008 disciplinano in maniera puntuale i diversi procedimenti amministrativi che fanno capo all'Ufficio. In questo quadro, il ricorso, ricondotto alla sua essenza propria, è lo strumento specifico per la tutela dei diritti di cui all'art. 7 del Codice e non l'indifferenziato mezzo per "provocare" comunque un pronunciamento dell'Autorità su ogni aspetto attinente alla protezione dei dati personali. Ciò spiega anche l'attenzione che l'Unità ricorsi riserva all'esame preliminare dei ricorsi che pervengono. In tale fase, infatti, l'Ufficio verifica con attenzione (oltre ai profili di tipo formale) l'effettiva riconducibilità delle

situazioni fatte valere al catalogo dei diritti di cui al citato art. 7 del Codice. Tuttora è agevole constatare come, nonostante gli anni trascorsi e l'ampia diffusione data alle decisioni del Garante, molti atti proposti nominalmente come "ricorsi" rappresentino invece mere segnalazioni su generiche violazioni delle disposizioni in materia di protezione dei dati personali, che spesso vengono accompagnate da richieste che esorbitano addirittura dall'ambito di competenza dell'Autorità (quali quelle di risarcimento del danno, o di pubblicazione di una "rettifica" ai sensi della cd. "legge sulla stampa", nell'ambito di segnalazioni in materia di trattamento a fini giornalistici, o le eccezioni di tipo squisitamente contrattuale, o sollevate a latere dei profili di protezione dei dati).

A fianco dei variegati strumenti di tutela che fanno capo al Garante, si colloca poi, con un numero sempre più elevato di casi che vengono comunque portati a conoscenza dell'Autorità, l'intervento dell'autorità giudiziaria ordinaria adita ai sensi dell'art. 152 del Codice (norma oggetto di una recente novella legislativa sulla quale, v. par. 2.1.6.).

Le forme di tutela della protezione dati tendono quindi a dilatarsi e a diffondersi sempre di più. L'azione specifica di tutela svolta dall'Autorità non è più, quindi, un elemento isolato, quasi anomalo nel generale panorama delle tutele (come poteva apparire agli albori della disciplina) ma si caratterizza come un'azione senza dubbio specializzata, ma ormai non più isolata in un contesto (quale quello della fine del secolo scorso) non ancora pronto a recepire il portato innovativo della l. n. 675/1996 e dei suoi successivi sviluppi. Da ciò, ovviamente, anche il moltiplicarsi dei pronunciamenti da parte dei tribunali, e di conseguenza l'esigenza di giungere ad un'interpretazione uniforme delle disposizioni più controverse attraverso l'intervento della Suprema Corte di Cassazione.

15.4. LE RECENTI MODIFICHE NORMATIVE

Sempre al fine di valutare l'influsso sul contenzioso proposto dinanzi all'Autorità, non si può non fare cenno alle recenti modifiche normative che hanno interessato il Codice in materia di protezione dei dati personali. Nel 2011 diversi interventi (tutti con lo strumento della decretazione d'urgenza) agendo, in alcuni casi anche ripetutamente, su alcune disposizioni quali gli artt. 4 e 5, hanno modificato in modo significativo il campo di

applicazione della legge. Ne è derivata, a partire dal d.l. 6 dicembre 2011, n. 201 la sottrazione in buona misura delle persone giuridiche dal campo di applicazione del Codice (cfr. al riguardo par. 2.1.1.). Le conseguenze sull'ambito di operatività dei ricorsi si sono immediatamente manifestate portando alla declaratoria di inammissibilità di diversi ricorsi proposti da persone giuridiche (in particolare società).

Va osservato al riguardo che proprio negli ultimi anni erano andati aumentando i ricorsi proposti da società commerciali, specie con riferimento ai dati personali trattati da istituti di credito nonché in relazione alle informazioni oggetto di raccolta e rielaborazione ad opera delle società operanti nel settore delle informazioni commerciali.

Si può quindi constatare che, a fronte di alcuni sgravi in tema di informativa e consenso, una nutrita e piuttosto significativa platea di soggetti ha perso la possibilità di attivare strumenti di tutela molto utili, specie quando sono in gioco informazioni rilevanti concernenti la reputazione stessa delle imprese.

15.5. TIPOLOGIA DI DECISIONI E CATEGORIE DI TITOLARI

L'esame delle tabelle statistiche in raffronto all'anno precedente consente di svolgere qualche ulteriore considerazione.

Per quanto riguarda la tipologia di decisioni adottate non emergono, in termini percentuali, scostamenti significativi. Si conferma come più del 50% dei ricorsi proposti si sia concluso con una declaratoria di "non luogo a provvedere". Ciò attesta l'efficacia dell'intervento dell'Autorità che, nel corso dell'istruttoria, in molti casi, induce e favorisce, anche prima della decisione finale, la positiva conclusione del procedimento.

Non meno significative, peraltro, le non irrilevanti percentuali di decisioni di infondatezza e di inammissibilità. Ancora una volta questo tipo di conclusione del procedimento attesta la tendenza a utilizzare la "scorciatoia" del ricorso quale strumento per provocare l'intervento del Garante anche in ambiti e situazioni nei quali non vi è spazio per questo strumento di tutela.

Anche per quanto riguarda le categorie di titolari del trattamento non si sono registrati nel 2011 significativi scostamenti rispetto agli anni immediatamente precedenti. Il settore bancario e finanziario (da intendersi nella sua più vasta accezione) si è confermato l'ambito

nel quale si è concentrata la maggior parte dei procedimenti. Ciò, sia con riguardo a ricorsi mirati ad acquisire elementi conoscitivi (ad esempio, accesso ai dati richiesto per ridefinire complesse vicende contrattuali o per acquisire elementi utili nell'ambito di controversie successorie) sia con riferimento alle numerose situazioni in cui è invece in discussione la divulgazione di dati negli archivi dei sistemi di informazioni creditizie o nell'archivio della Centrale d'allarme interbancaria (Cai) o l'inserimento di dati nei report diffusi dalle società specializzate nel settore dell'informazione commerciale. Peraltro, la varietà dei settori lambiti dai ricorsi è vastissima, passando, come detto, dall'attività dei soggetti pubblici e delle strutture sanitarie (anche private), ai trattamenti svolti in ambito giornalistico, al variegato ambito del *marketing* (visto essenzialmente attraverso i molteplici ricorsi proposti per tutelare il diritto di opposizione alle comunicazioni pubblicitarie indesiderate).

15.6. LA CASISTICA PIÙ SIGNIFICATIVA

Si segnalano in questa sezione alcuni settori rispetto ai quali, durante l'anno 2011, significative decisioni hanno contribuito a "fissare" o consolidare orientamenti interpretativi del Garante degni di attenzione.

Trattamento dati nell'ambito dei cd. "archivi *online*"

Si tratta di un "filone" di procedimenti di estremo interesse e delicatezza sul quale negli ultimi tre anni il Garante ha più volte richiamato l'attenzione. La sempre più ampia disponibilità gratuita sulla rete internet di archivi storici di quotidiani e periodici, unita alle straordinarie capacità di indicizzazione dei motori di ricerca, ha portato a far "riaffiorare" in modo automatico un'infinità di notizie che potevano ormai considerarsi coperte dall'oblio. Da ciò, la naturale reazione di molti interessati (protagonisti di fatti di cronaca, parenti ed eredi degli stessi, vittime di reato, ecc.) che, visti riemergere aspetti e momenti generalmente negativi della propria vita, hanno reagito proponendo, in prima battuta, istanze di blocco e cancellazione dei dati rinvenuti nei nuovi archivi della memoria digitale, e sollecitando almeno "l'attenuazione" degli effetti moltiplicatori (in termini di consultabilità delle informazioni) indotti dall'azione dei motori di ricerca generalisti. Il Garante anche nel corso del 2011 ha preso posizione più volte su tali aspetti (per i quali v. anche par. 7.5.) con una serie di decisioni nelle quali si evidenziano i seguenti orientamenti.

1) Il trattamento di dati connesso alla diffusione negli archivi storici accessibili *online* dei contenuti giornalistici a suo tempo divulgati per il tramite delle tradizionali edizioni cartacee è da considerarsi lecito. L'originario trattamento svolto per fini giornalistici rientra ora tra i trattamenti effettuati per fini di conservazione della memoria storica. Tale ulteriore finalità, per espressa previsione normativa (art. 99, comma 1, del Codice), è considerata compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.
2) Di conseguenza, sono state giudicate infondate le istanze volte ad ottenere la cancellazione dei dati, di tipo "negativo" eventualmente contenuti negli articoli, anche molto risalenti nel tempo, ora riprodotti nei nuovi archivi *online*, ferma restando naturalmente la possibilità di esercitare le azioni a tutela dei profili concernenti l'onore e la reputazione eventualmente lesi per effetto degli articoli medesimi.
3) Il Garante ha invece accolto in più occasioni la richiesta volta ad interdire l'indicizzazione dei dati, ad opera dei più diffusi motori di ricerca esterni al sito internet sorgente nel quale tali informazioni sono ora riportate. In questo modo le informazioni vengono conservate nella loro integrità nel sito del giornale che a suo tempo le aveva pubblicate ma non sono direttamente e facilmente raggiungibili da chi operi (quasi sempre a tutt'altro fine) una generica ricerca in rete di informazioni relative ad una certa persona. Questa possibilità di "deindicizzazione" ha dato finora buona prova, contribuendo a risolvere in via di fatto molte situazioni delicate ed ha trovato ormai un diffuso consenso anche da parte degli editori. È facile constatare, infatti, come ormai molte richieste di questo tipo vengono accolte subito dopo la presentazione dell'interpello preventivo, senza arrivare neanche all'instaurazione di un ricorso formale.
4) La soluzione prospettata deve naturalmente essere calata nel variegato contesto dei casi che in concreto possono presentarsi. Le richieste di deindicizzazione sono così state prese in considerazione con riferimento alle segnalazioni ed ai ricorsi pervenuti, ad esempio, da persone non note, da vittime di reato, da terzi citati in relazione a fatti di cronaca incentrati su diversi protagonisti, tenendo ovviamente presente soprattutto il decorso di un significativo lasso di tempo dalla originaria pubblicazione, tale da

giustificare il consolidarsi di un naturale oblio su tali vicende. La soluzione prospettata mira a contemperare valori e princìpi costituzionalmente rilevanti ma potenzialmente confliggenti nelle fattispecie concrete: la tutela della dignità e della riservatezza delle persone e, in particolare, la possibilità di salvaguardare una identità personale "ricostruita" (magari dopo traversie ed errori), il diritto alla libera informazione su fatti e vicende di interesse pubblico, il diritto alla libera ricerca (in particolare storica) che ovviamente postula la possibilità di disporre (in modo facilmente accessibile) della maggior quantità possibile di fonti e di documenti.

A testimonianza dell'importanza del tema e della sua attualità è facile constatare come sul problema del cd. "diritto all'oblio" connesso alla divulgazione giornalistica delle informazioni si sono infittiti nel giro di pochi anni gli interventi giornalistici, le sentenze dei giudici, il dibattito della dottrina. In questo contesto è attesa la decisione della Cassazione avverso la sentenza del Tribunale di Milano n. 4302/2010 del 6 aprile 2010 che aveva respinto l'impugnazione della deliberazione del Garante con cui era stata rigettata la richiesta dell'interessato di rendere non reperibile attraverso i comuni motori di ricerca, in quanto non aggiornato, un articolo che informava di procedimenti giudiziari a suo carico senza dar notizia degli sviluppi a lui favorevoli.

Trattamento dati in ambito giornalistico

Anche nel 2011 sono stati diversi i pronunciamenti su vari aspetti del trattamento dati in ambito giornalistico. Al riguardo, su un piano generale, è facile constatare come sempre più spesso i ricorsi su questa materia facciano riferimento a forme non tradizionali di giornalismo o all'utilizzo di strumenti innovativi che arricchiscono le classiche fonti dell'attività informativa. Rilevano in particolare, l'attività giornalistica svolta attraverso appositi siti internet o comunque attraverso l'offerta in rete di contenuti informativi, il preponderante utilizzo di immagini e suoni digitalizzati che dànno immediatezza alla notizia stessa, superando tutte le barriere e le mediazioni prima esistenti, il ruolo sempre più attivo, specie in ambito televisivo, del giornalismo d'inchiesta, con modalità volte anche alla raccolta "di sorpresa" delle informazioni, facilitata dalle nuove tecnologie.

Questa evoluzione dell'attività giornalistica è testimoniata da alcune decisioni adottate nel 2011, pur nell'estrema varietà delle situazioni ed anche nell'oggettivo, differente rilievo dei diritti in gioco.

Con provvedimento del 7 luglio 2011 [doc. *web* n. 1834934] il Garante ha parzialmente accolto le richieste di alcuni esponenti locali di una formazione politica che avevano lamentato la diffusione su un periodico *online*, nell'ambito di una più ampia cronaca sulle divisioni all'interno del partito, di numerosi scambi di e-mail fra i ricorrenti. Pur riconoscendo che lo scambio di corrispondenza elettronica rimandava a considerazioni già pubblicamente espresse dai medesimi interessati e faceva comunque riferimento allo svolgimento di attività politica, il Garante ha ritenuto che tale integrale pubblicazione dei messaggi (comprensiva anche degli indirizzi di posta elettronica) fosse eccedente rispetto alle finalità perseguite e non rispettosa del principio dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico. Da ciò la decisione di ordinare la rimozione di tali dati dal sito in questione.

Significativa anche la decisione del 24 novembre 2011 [doc. *web* n. 1870903] con la quale è stato dichiarato infondato il ricorso proposto da un'attrice citata nell'ambito della trascrizione di un'intercettazione telefonica relativa ad un colloquio fra un noto esponente politico e un dirigente della Rai. Il Garante, nel rilevare che le informazioni erano state acquisite lecitamente, ha sottolineato l'esistenza di un interesse pubblico alla conoscenza della vicenda, oggetto di un'indagine giudiziaria diretta a individuare anche eventuali favoritismi nei confronti di personaggi del mondo dello spettacolo.

All'ambito del giornalismo d'inchiesta si riconnette il provvedimento del 30 dicembre 2011 [doc. *web* n. 1873945] che, nel ritenere lecito il trattamento di dati svolto in occasione di riprese televisive effettuate, senza preavviso, in luogo pubblico in relazione ad una vicenda di rilevante interesse sociale, ha però accolto la richiesta di una persona, ripresa e intervistata "di sorpresa", che si opponeva all'ulteriore trattamento della propria immagine (attesa la perdurante diffusione della trasmissione sul sito internet della stessa). Ciò, sia in considerazione della non notorietà della persona sia dell'irrilevanza della sua diretta identificazione rispetto alle finalità informative ancora rinvenibili in un servizio andato in onda alcuni mesi prima. Si è pertanto ordinato all'editore di adottare le misure idonee a non consentire la riconoscibilità dell'interessata (tramite oscuramento del volto).

In una prospettiva più tradizionale rientra il caso deciso il 26 ottobre 2011 [doc. *web* n. 1855372], incentrato sulle modalità con le quali si era data evidenza a due vicende di cronaca

che avevano visto involontario protagonista il ricorrente. In particolare, con riferimento alla descrizione di un furto perpetrato ai suoi danni, il Garante ha accolto la richiesta rivolta all'editore di astenersi da qualunque ulteriore trattamento di alcuni dati specifici (nominativo per esteso e indirizzo completo di residenza). Ciò specie in riferimento all'eventuale pubblicazione *online* degli articoli in questione che rischierebbe di moltiplicare il rilievo negativo delle vicende descritte.

Trattamento di dati personali nell'ambito del rapporto di lavoro

Come segnalato nelle pagine precedenti (cfr. par. 10.), la realtà del lavoro dipendente, pubblico e privato, ha dato luogo negli ultimi tempi ad un crescente numero di procedimenti nei quali le richieste di intervento sui dati personali si inseriscono, in modo sempre più pregnante, in contenziosi più ampi, normalmente incentrati su procedimenti disciplinari in itinere o su ricorsi avverso provvedimenti di licenziamento già adottati, nonché in vicende legate alla valutazione delle performance dei singoli dipendenti.

A quest'ultimo filone sono riconducibili le decisioni di accoglimento, per i dati non ancora forniti all'interessato, a seguito di due ricorsi decisi il 15 giugno 2011 [doc. *web* nn. 1829925 e 1827162] concernenti un'ampia richiesta di dati personali relativi a due dipendenti di un istituto di credito, specificamente incentrata sulle mansioni svolte, sulle valutazioni di anno in anno ricevute, sui corsi di formazione frequentati.

Nella stessa prospettiva si collocano anche le decisioni "di non luogo a provvedere", per l'intervenuta comunicazione dei dati richiesti dall'interessato del 6 dicembre 2011 [doc. *web* n. 1872740], sulla richiesta di accesso alla scheda di valutazione delle prestazioni relativa all'anno 2007 e del 15 dicembre 2011 [doc. *web* n. 1876777], sulla richiesta di conoscere tutti gli elementi di dettaglio di un elaborato programma aziendale di valutazione delle prestazioni.

Con il provvedimento del 15 dicembre 2011 [doc. *web* n. 1876784] il Garante ha poi riconosciuto la legittimità dell'attività investigativa svolta da apposita agenzia nei riguardi di un informatore scientifico del farmaco che aveva poi dato luogo ad un provvedimento disciplinare. Ferme restando le valutazioni proprie del giudice nella controversia di lavoro, è stato peraltro riconosciuto il diritto dell'interessato a conoscere le informazioni raccolte sul proprio conto dagli investigatori privati.

Particolarmente complessa e delicata la vicenda decisa il 6 dicembre 2011 [doc. *web* n. 1872753] relativa al trattamento di dati sensibili attinenti alla vita sessuale, utilizzati da un ente pubblico per promuovere un procedimento disciplinare a carico di un proprio dipendente. Sulla base della ricostruzione normativa effettuata, con specifico riferimento all'assenza di specifici richiami nel regolamento per il trattamento dei dati sensibili e giudiziari dell'ente in questione, il Garante ha ritenuto illecito il trattamento effettuato (attraverso l'acquisizione di dati e fotografie su siti internet), vietando pertanto all'ente stesso di trattare ulteriormente tali informazioni.

16. IL CONTENZIOSO GIURISDIZIONALE

16.1. CONSIDERAZIONI GENERALI

Anche nel 2011 è stata confermata l'utilità 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 135 ricorsi del 2010, sono stati trattati dall'Autorità 170 ricorsi relativi a giudizi proposti nel 2011 non coinvolgenti direttamente pronunce del Garante.

Per l'elevato numero di tali controversie, assume sempre maggiore rilevanza l'obbligo –purtroppo non sempre puntualmente adempiuto– per le cancellerie, di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6,). Vi è inoltre da osservare che l'autorità giudiziaria continua a ritenere necessaria la notifica al Garante dei ricorsi ad essa presentati, *ex* art. 152 del Codice, benché il comma 7 dello stesso articolo, che prevedeva esplicitamente tale obbligo, sia stato abrogato dall'art. 34 del d.lgs. n. 150/2011, il cui art. 10, comma 1, salva diversa disposizione, sottopone al rito del lavoro le controversie previste dal medesimo art. 152 (cfr. par. 2.1.6.).

Tali strumenti consentono al Garante di avere un'ampia informazione sull'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo gli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

16.2. I PROFILI PROCEDURALI

L'art. 152 devolve tutte le controversie riguardanti l'applicazione del Codice all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento (art. 10, comma 2, del d.lgs. n. 150/2011).

In tema di giurisdizione, la Corte di Cassazione a sezioni unite ha definito una controversia inerente all'impugnazione del silenzio-rifiuto del Garante sulla richiesta di una società che gestisce un sistema di informazione creditizia, di fissare l'importo del contributo,

previsto dall'art. 10, commi 7 e 8, del Codice, che il titolare può richiedere agli interessati per l'attività volta a corrispondere alle richieste di accesso e comunicazione dei dati personali.

Sia il Tribunale amministrativo regionale del Lazio (sentenza n. 587 del 3 dicembre 2008) sia il Consiglio di Stato (sentenza n. 5198 del 3 settembre 2009) avevano affermato la propria giurisdizione. In particolare, il Consiglio di Stato aveva sostenuto che l'art. 152 non attribuisce al giudice ordinario la cognizione su interessi legittimi, confermando il tradizionale criterio di riparto di giurisdizione, fondato sulla distinzione tra diritti e interessi legittimi. Nella specie, la società avrebbe vantato un mero interesse legittimo alla fissazione del contributo da parte del Garante, con conseguente giurisdizione del giudice amministrativo.

La Suprema Corte, adita dal Garante con ricorso, ai sensi dell'art. 360, comma 1, n. 1, c.p.c., ha invece ritenuto, come sostenuto dall'Autorità, che la giurisdizione nel caso di specie dovesse essere attribuita al giudice ordinario, così come disposto dall'art. 152 del Codice, "la cui cristallina espressione letterale (*rara avis*) non lascia margini a dubbi circa l'*intentio legis* di attribuire l'intera materia alla cognizione dell'AGO", essendo peraltro "anche all'autorità giudiziaria consentito, per effetto di conforme disposizione del legislatore ordinario, di conoscere di interessi legittimi (...)" (sentenza n. 8487 del 14 aprile 2011).

Ancora in tema di giurisdizione, a fronte dell'opposizione proposta da un ministero ad una contestazione di violazione amministrativa, il Tribunale amministrativo regionale del Lazio ha dichiarato il proprio difetto di giurisdizione in favore del giudice ordinario, facendo corretta applicazione del dettato dell'art. 152, comma 1, del Codice (sentenza n. 10161 del 13 dicembre 2011).

16.3. I PROFILI DI MERITO

Analogamente a quanto verificatosi nello scorso anno, alcune pronunce emesse dall'autorità giudiziaria, in fattispecie in cui non erano in discussione provvedimenti adottati dal Garante, hanno riguardato il trattamento dei dati personali effettuato da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti, confermando che si tratta di un profilo di grande importanza per gli interessati, e che frequentemente genera contenzioso.

I giudizi hanno riguardato, in particolare, segnalazioni degli interessati come cattivi pagatori da parte di istituti di credito o società finanziarie ai soggetti che gestiscono i Sistemi di informazioni creditizia (Sic).

In tre casi la segnalazione è stata riconosciuta non corretta, con condanna dell'istituto bancario che l'aveva effettuata al risarcimento del danno in favore dell'interessato. I tre casi concernono: un correntista segnalato dalla propria banca in relazione ad una posizione debitoria di sofferenza il cui importo era stato oggetto di contestazione da parte del debitore –che al riguardo aveva anche ottenuto una sentenza favorevole– e che non doveva considerarsi espressione di una sua effettiva incapacità patrimoniale (Tribunale di Napoli, sezione distaccata di Casoria, sentenza del 28 gennaio 2011); il sottoscrittore di una proposta di abbonamento per l'installazione di un'apparecchiatura, con contestuale proposta di finanziamento, che aveva tempestivamente esercitato il diritto di recesso (Tribunale di Tempio Pausania, sezione distaccata di La Maddalena, sentenza n. 811 del 26 novembre 2011); un soggetto erroneamente segnalato da una banca in relazione ad una garanzia reale, in realtà mai costituita, gravante sul suo patrimonio in favore di un terzo. In questo caso l'istituto ha riconosciuto il proprio errore e ha provveduto spontaneamente a rettificare la posizione dell'interessato, in data antecedente alla presentazione del ricorso, con effetti retroattivi (Tribunale di Torino, sentenza n. 360 del 19 gennaio 2011).

Nei primi due casi gli enti resistenti oltre che al risarcimento del danno sono stati condannati anche alla cancellazione dei dati personali dei ricorrenti.

In otto casi il ricorso è stato respinto in relazione alla segnalazione: dell'amministratore di una società, autorizzato ad emettere assegni per la stessa, a seguito della cessazione da tale carica e della indebita compilazione da parte dei soci di un assegno da lui sottoscritto in bianco, non potendo nella specie essere imputata alla banca l'illegittima segnalazione (Tribunale di Roma, sentenza n. 508 del 12 gennaio 2011); del sottoscrittore di un contratto di finanziamento per l'acquisto di un bene, in relazione al quale l'interessato non aveva validamente esercitato il diritto di recesso (Tribunale di Milano, sentenza n. 5478 del 31 agosto 2011); di un soggetto che, in un caso analogo al precedente, aveva sostenuto di aver esercitato il diritto di recesso in riferimento ad un contratto di finanziamento per

l'acquisto di un corso di lingua; il Tribunale di Milano ha ritenuto legittima la segnalazione al Sic da parte della società finanziaria in virtù degli accordi intervenuti con la società venditrice del corso (sentenza n. 5042 del 12 aprile 2011); di un soggetto riferita al rifiuto di una richiesta di finanziamento da parte di un istituto di credito, in quanto, in base alla normativa vigente, l'ente erogatore può richiedere l'iscrizione presso la banca dati anche delle richieste di finanziamento, indipendentemente dal loro esito (Tribunale di Milano, sentenza n. 419 del 13 gennaio 2011); del sottoscrittore di un contratto di finanziamento estinto anticipatamente, risultato moroso in base ad una precedente sentenza emessa dal Giudice di pace di Taranto (Tribunale di Milano, sentenza n. 14222 del 22 novembre 2011); di un soggetto a cui erano stati imputati ritardi nei pagamenti di rate di prestiti poi regolarizzati con successiva chiusura del finanziamento; il Tribunale di Milano ha ritenuto il comportamento della società finanziaria conforme alle disposizione che regolano la materia, in tema di termini entro i quali le informazioni creditizie di tipo negativo possono essere conservate nel Sic (sentenza n. 5535 del 20 aprile 2011); di un soggetto, in conseguenza di un errore di identificazione; il Tribunale di Milano ha riscontrato che la società sulla base degli atti in suo possesso aveva ottemperato ai doveri di diligenza nell'accertamento dell'identità dell'apparente debitore, tenuto conto che l'ente finanziatore non ha un rapporto diretto con il cliente (Tribunale di Milano, sentenza n. 9240 dell'8 luglio 2011); di una società insolvente rispetto ad un credito che altra società aveva ceduto pro soluto alla resistente. Il Tribunale di Milano ha statuito che, nel caso di specie, la società di *factoring* resistente aveva legittimamente proceduto alla segnalazione della debitrice secondo quanto previsto dalla relativa normativa, in considerazione della condizione di sofferenza, essendo irrilevante che non sussistesse un rapporto di finanziamento diretto fra le parti (sentenza n. 114332 del 6 ottobre 2010).

In due casi, entrambi decisi dal Tribunale di Milano, i ricorsi hanno riguardato il preavviso di segnalazione ad un Sic, che cui il titolare del trattamento, partecipante al sistema di informazioni creditizie, è tenuto, a fornire all'interessato al verificarsi di ritardi nei pagamenti.

In entrambi i casi il tribunale ha accertato l'inadempimento a tale obbligo da parte delle società finanziarie convenute, che non avevano fornito alcun riscontro sul ricevimento del

preavviso, ma ha respinto le domande di risarcimento per difetto di prova dell'esistenza del danno (sentenza n. 5471 del 19 aprile 2011 e sentenza n. 11549 del 29 settembre 2011).

16.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2011 ha registrato un incremento delle opposizioni a provvedimenti del Garante: a fronte dei 65 ricorsi del 2010, nel 2011 sono state proposte 72 opposizioni. Di queste, 45 si riferiscono a opposizioni a ordinanze ingiunzioni, con un netto aumento rispetto al 2010, nel quale si erano registrate 19 opposizioni di tale natura.

Complessivamente l'Autorità ha avuto notizia di 39 decisioni dell'autorità giudiziaria relative ad opposizioni a provvedimenti del Garante che, con due sole eccezioni, si è sempre costituito in questi giudizi.

Dodici pronunce hanno riguardato opposizioni a ordinanze ingiunzioni. Sei hanno avuto a oggetto violazioni dell'art. 13 del Codice per omessa o inidonea informativa agli interessati.

Tre di queste pronunce, riguardanti trattamenti di dati svolti, rispettivamente, attraverso l'attività di *marketing* da parte di un centro didattico, la compilazione di form sul sito internet da parte di una società che gestisce strutture turistiche e la gestione di un impianto di videosorveglianza da parte di una società produttrice di prodotti professionali, hanno respinto le opposizioni, confermando i provvedimenti del Garante (Tribunale di Rimini, sentenza n. 891 del 21 luglio 2011; Tribunale di Tempio Pausania, sentenza n. 41 del 17 febbraio 2011; Tribunale di Varese, sentenza n. 1609 del 23 dicembre 2010).

In un caso, la sanzione è stata ridotta a causa del grado della colpa, ritenuto lieve, nella condotta di una società, che somministra servizi di *beauty farm*, la quale non aveva rilasciato la dovuta informativa ai propri clienti (Tribunale di Genova, sentenza n. 546 del 4 febbraio 2011).

In due casi il ricorso è stato proposto avverso il verbale di contestazione di violazione amministrativa.

In sintonia con il consolidato orientamento della Corte di Cassazione, cui il Garante aderisce, in entrambi i casi, concernenti l'omessa informativa agli interessati e la mancata acquisizione del loro consenso (artt. 13 e 23 del Codice), i ricorsi sono stati dichiarati

inammissibili, non essendo la contestazione autonomamente impugnabile, non costituendo decisione finale del Garante sulla irrogazione della sanzione, costituita dalla eventuale ordinanza ingiunzione (Tribunale di Roma, sentenza n. 8175 del 19 aprile 2011; Tribunale di Torino, sentenza n. 868 del 9 febbraio 2011).

Un'opposizione è stata accolta dal Tribunale di Palmi, Sez. distaccata di Cinquefondi, il quale ha ritenuto che le immagini raccolte attraverso un sistema di videosorveglianza posto all'ingresso di un esercizio commerciale, attese le specifiche modalità della loro acquisizione, limitate nel tempo e nelle finalità, non costituiscano dato personale in grado di veicolare alcuna portata informativa relativa alle persone riprese (sentenza n. 205 del 17 maggio 2011).

Avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Tre pronunce hanno avuto a oggetto la violazione degli artt. 37 e 38 del Codice per omessa o incompleta notificazione.

Due casi hanno riguardato società che trattano dati sanitari, mentre il terzo caso verteva in materia di trattamento dati biometrici da parte di un datore di lavoro. Tutte le decisioni hanno respinto le opposizioni, confermando i provvedimenti del Garante (Tribunale di Roma, sentenza n. 18324 del 22 settembre 2011; Tribunale di Prato, sentenza n. 964 del 19 settembre 2011; Tribunale di Ancona, sentenza n. 1704 del 3 novembre 2010).

Due pronunce hanno avuto a oggetto il mancato rispetto da parte del Garante del termine di novanta giorni dall'accertamento, entro il quale deve avvenire la notificazione della contestazione di violazione amministrativa (sul punto v. anche par. 17.4.3.).

Un'opposizione è stata respinta (Tribunale di Milano, sentenza n. 11545 del 30 settembre 2011), mentre l'altra è stata accolta (Tribunale di Roma, sentenza n. 21632 del 3 novembre 2011).

La mancata adozione di una misura minima di sicurezza, consistente nell'omessa designazione di un incaricato del trattamento da parte di un comune in violazione dell'art. 30 del Codice, è stata oggetto della sentenza del Tribunale di Cosenza, che ha dichiarato inammissibile il ricorso, sulla considerazione che il provvedimento impugnato non è un'ordinanza ingiunzione, come ritenuto del ricorrente, ma una prescrizione impartita dal Garante, che costituisce atto interno del procedimento penale instaurato ai sensi dell'art. 169 del Codice nei confronti dell'autore della violazione (sentenza n. 1090 dell'8 luglio 2011).

In tema di violazione della disciplina inerente al necessario previo consenso al trattamento dei dati, si sono avute 5 pronunce, 4 delle quali hanno confermato i provvedimenti del Garante.

Nel primo caso, il Tribunale di Roma ha confermato il provvedimento del 26 novembre 2009 (doc. *web* n. 1681825) con cui il Garante aveva inibito a una società che opera nel mercato dei prodotti e servizi di *marketing* l'uso e la comunicazione a terzi dei dati personali degli interessati, in quanto la società aveva raccolto le informazioni acquisendo dagli interessati un unico consenso generale e non, come dovuto, separati consensi in relazione ad ogni distinto trattamento effettuato (sentenza n. 19281 del 5 ottobre 2011).

Nel secondo caso, il Tribunale di Venezia, conformemente a quanto deciso dal Garante con il provvedimento del 4 novembre 2010 (doc. *web* n. 1767785), ha dichiarato illecito il trattamento dei dati personali effettuato da una società operante nell'ambito del *telemarketing* poiché la normativa prevede che, in caso di uso di sistemi automatizzati di chiamata senza l'intervento di un operatore (art. 130, comma 1, del Codice), possono essere utilizzate banche dati costituite sulla base di elenchi pubblici formati prima del 1° agosto 2005 solo con il consenso specifico degli interessati, che la società non aveva acquisito (sentenza n. 10 del 14 ottobre 2011).

Nella terza pronuncia, il giudice ha confermato il provvedimento del Garante del 27 maggio 2010 (doc. *web* n. 1738383) nella parte in cui ha dichiarato illegittima la comunicazione effettuata da una casa di cura dei risultati di accertamenti diagnostici per infezione da HIV al medico curante dell'interessato, in assenza del consenso espresso di questi (Tribunale di Padova, sentenza n. 3 del 2 febbraio 2011).

Nella quarta, il Tribunale di Taranto ha ritenuto infondato il ricorso di un interessato che aveva chiesto la cancellazione dei propri dati personali sulla denunzia di un contratto verbale di locazione registrato dall'Agenzia delle entrate, in quanto la registrazione sarebbe stata effettuata senza suo consenso.

Confermando il provvedimento del Garante del 14 aprile 2011 (doc. *web* n. 1816371), il Tribunale ha ritenuto che l'Agenzia delle entrate aveva trattato i dati nell'assolvimento dei suoi fini istituzionali e quindi, in quanto soggetto pubblico, non era sottoposta all'obbligo di richiedere il consenso dell'interessato (sentenza n. 2098 del 28 ottobre 2011).

Nell'ultima decisione, il Tribunale di Trento ha accolto il ricorso presentato da una banca avverso il provvedimento del Garante del 18 marzo 2010 (doc. *web* n. 1715015), che aveva dichiarato illecito il trattamento dei dati effettuato dall'istituto, tramite l'accesso di un suo dipendente ai dati bancari riferiti al ricorrente, in assenza del suo consenso, prescrivendo contestualmente di rafforzare le misure di sicurezza nella protezione delle informazioni. Tale accesso aveva consentito la comunicazione dei dati a un terzo.

Il giudice ha ritenuto che il consenso reso dall'interessato alla banca al trattamento dei suoi dati personali all'inizio del rapporto vale per ogni successivo trattamento, mentre non era risultata provata la comunicazione dei dati a terzi (sentenza n. 153 del 23 febbraio 2011).

Avverso tale pronuncia, l'Autorità ha proposto ricorso per Cassazione.

Per quanto attiene al trattamento di dati personali effettuato in ambito giornalistico, vanno segnalate 2 pronunce. In entrambi i casi l'Autorità, con i provvedimenti del 14 gennaio 2010 e del 12 febbraio 2009, aveva respinto i ricorsi volti ad ottenere la cancellazione dei dati personali contenuti in alcuni articoli consultabili, anche in versione informatica, nell'archivio storico di un noto quotidiano (doc. *web* nn. 1701524 e 1601624).

Il Tribunale di Milano ha confermato l'orientamento del Garante, secondo il quale il trattamento dei dati effettuato dal quotidiano mediante l'inserimento degli articoli nell'archivio della testata giornalistica era legittimato da finalità storiche (sentenza n. 12004 dell'11 ottobre 2011 e sentenza n. 3950 del 7 aprile 2011).

In un altro caso, relativo alla pubblicazione sul sito internet del Senato di un atto di sindacato ispettivo contenente dati personali del ricorrente, il Tribunale di Roma, nell'accogliere l'opposizione al provvedimento del 16 luglio 2009 con cui il Garante aveva dichiarato inammissibile il ricorso (doc. *web* n. 1638472), ha disposto che i dati personali del ricorrente non siano reperibili attraverso i comuni motori di ricerca, ma solo mediante l'accesso al sito istituzionale (sentenza n. 21961 del 9 novembre 2011).

Due sentenze hanno avuto a oggetto il provvedimento del 6 novembre 2008, n. 60 con cui il Garante, constatata la conformità alle leggi e ai regolamenti, ha disposto la trasmissione del "Codice di deontologia e di buona condotta per il trattamento dei dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria" (doc. *web* n. 1565171) al Ministro della giustizia per la sua pubblicazione sulla Gazzetta Ufficiale.

Entrambe le pronunce hanno respinto l'opposizione, confermando la legittimità del provvedimento del Garante, avendo rilevato la conformità a leggi e regolamenti delle disposizioni del codice deontologico impugnate (Tribunale di Bassano del Grappa, sentenze nn. 751 e 752 del 21 dicembre 2010).

Tre pronunce hanno riguardato l'esercizio del diritto di accesso ai dati personali, previsto dall'art. 7, comma 1, del Codice.

In due casi, tale diritto è stato esercitato dagli eredi in relazione ai nominativi dei beneficiari di una polizza assicurativa sottoscritta dal *de cuius*.

Nel primo, l'opposizione proposta avverso il provvedimento del Garante del 10 dicembre 2009 (doc. *web* n. 1692945) è stata accolta, in quanto il Tribunale di Verona ha ritenuto che la qualità di erede legittimi il ricorrente ad esercitare il diritto di accesso a tutela dei propri diritti ereditari (sentenza n. 53 del 13 gennaio 2011).

Avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Nel secondo, il Tribunale di Roma, conformemente a quanto stabilito dal Garante con provvedimento del 26 luglio 2005 (doc. *web* n. 1157566), ha ritenuto che gli eredi hanno diritto ad ottenere, oltre alle informazioni riconducibili alla sfera personale del *de cuius*, anche i dati personali relativi a terze persone, senza il consenso di queste, solo nel caso, non ricorrente nella specie, in cui il trattamento sia necessario a far valere o difendere un diritto in sede giudiziaria (sentenza n. 5606 del 15 marzo 2011).

Un'ulteriore pronuncia ha confermato il provvedimento del Garante del 23 luglio 2009 (doc. *web* n. 1639928) che aveva condannato un'amministrazione pubblica al pagamento delle spese del procedimento amministrativo in favore del ricorrente, pur avendo disposto il non luogo a provvedere sul ricorso ai sensi dell'art. 149, comma 2, del Codice, in quanto l'amministrazione aveva dato riscontro alla richiesta di accesso solo dopo l'intervento del Garante, sollecitato dall'interessato (Tribunale di Lecce, sentenza n. 208 del 25 febbraio 2011).

Sette sentenze hanno avuto a oggetto la violazione dell'art. 7, comma 3, del Codice, relativamente al diritto degli interessati di ottenere l'aggiornamento e la cancellazione dei dati che li riguardano contenuti in banche dati.

Tre di queste hanno interessato la medesima società che tratta i dati per finalità di informazione commerciale.

Nella prima, in cui si verteva in tema di mancato aggiornamento di un pignoramento, il giudice ha, in primo luogo, dichiarato inammissibile il ricorso nei confronti del presunto silenzio rigetto del Garante, che sul ricorso dell'interessato aveva pronunciato tempestivamente, con il provvedimento del 29 ottobre 2009, non impugnato nei termini (doc. *web* n. 1681825). Nel merito, pur ritenendo che il trattamento dei dati effettuato dalla società non fosse stato conforme alle previsioni del Codice, ha rigettato la richiesta di risarcimento del danno avanzata dall'interessato, perché non provata (Tribunale di Milano, sentenza n. 1404 del 1° febbraio 2011).

Le ulteriori due pronunce hanno riguardato il caso della diretta associazione alle persone degli interessati dell'informazione relativa alla dichiarazione di fallimento di una società in cui gli stessi avevano rivestito cariche societarie.

In un caso, il tribunale ha respinto l'opposizione al provvedimento del Garante dell'11 febbraio 2010 (doc. *web* n. 1705084), sostenendo la non pertinenza dell'informazione relativa al fallimento della società, soggetto terzo rispetto ai resistenti, a cui non possono essere addebitate responsabilità per le cariche ricoperte in epoca anteriore alla dichiarazione di fallimento (Tribunale di Milano, sentenza n. 4317 del 30 marzo 201).

Il Tribunale di Roma ha, invece, accolto l'opposizione al provvedimento del Garante del 29 aprile 2009 (doc. *web* n. 1617609), stabilendo che la qualifica di amministratore unico di una società fallita, rivestita dal resistente fino a meno di un anno prima del fallimento, sia pertinente con la finalità, perseguita dal titolare del trattamento, di fornire un'ampia informazione commerciale sulla solvibilità e affidabilità dei soggetti ai quali l'informativa si riferisce (sentenza n. 21380 del 28 ottobre 2011).

Con un'altra pronuncia, concernente il trattamento operato da una società che gestisce un sistema di informazioni creditizie, il Tribunale di Bologna ha confermato il provvedimento del Garante del 2 febbraio 2009 (doc. *web* n. 1597044), dichiarando che la richiesta del ricorrente, volta ad ottenere la cancellazione dal sistema delle informazioni che lo riguardano, non poteva essere accolta in quanto non era decorso il previsto termine di trentasei mesi previsto dal "Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti" (doc. *web* n. 1556693) (sentenza n. 1904 del 14 giugno 2011).

Una decisione ha riguardato l'accertamento dell'illegittimità della segnalazione del nominativo del ricorrente alla Centrale rischi della Banca d'Italia effettuato da una società finanziaria cessionaria di un credito nei confronti dell'interessato. Il Tribunale di Milano ha condiviso l'impostazione espressa dal Garante nel provvedimento del 5 marzo 2009 (doc. *web* n. 1608138), che aveva dichiarato inammissibile la richiesta di cancellazione della segnalazione in quanto non oggetto dell'interpello preventivo, e ha considerato come istanza di accertamento incidentale la domanda sulla legittimità della segnalazione, non essendo ammissibile chiedere al Garante il mero accertamento del diritto leso. Nel merito, il giudice ha respinto il ricorso, ritenendo corretto il comportamento della società resistente (sentenza n. 3856 del 21 marzo 2011).

Un'altra decisione ha confermato la legittimità del provvedimento del Garante del 7 ottobre 2009 (doc. *web* n. 1670167) che aveva ritenuto inammissibile il ricorso proposto, ai sensi degli artt. 7, commi 2 e 3 e 145 del Codice, nei confronti del Ministero dell'interno da un soggetto che aveva chiesto di conoscere l'origine dei dati che lo riguardano conservati presso il Centro elaborazione dati del Dipartimento della pubblica sicurezza del Ministero e l'eventuale cancellazione dei dati trattati in violazione di legge. Ai sensi degli artt. 8, comma 2, lett. *h*) e 53 del Codice, in questo ambito, infatti, i diritti di cui all'art. 7 non possono essere esercitati con la richiesta rivolta direttamente al titolare o al responsabile del trattamento e il successivo ricorso al Garante (Tribunale di Roma, sentenza n. 18834 del 27 settembre 2011).

Infine, un'ultima pronuncia ha accolto l'opposizione al provvedimento del Garante del 10 giugno 2011 (doc. *web* n. 1823181), ordinando ad una Conservatoria dei registri immobiliari la cancellazione delle trascrizioni a carico dell'interessato conservate nella propria banca dati a seguito dell'adempimento delle relative obbligazioni da parte del ricorrente (Tribunale di Milano, sentenza n. 280 del 12 gennaio 2012).

Una pronuncia ha riguardato un caso di trasferimento di dati per via telematica da parte di una società operante nel settore della consulenza per finalità promozionali a un noto operatore di telecomunicazioni, in base ad un accordo di *hosting*. Il provvedimento del Garante del 28 gennaio 2010 aveva vietato alla società di effettuare ulteriori trattamenti dei dati personali, in base alla circostanza che tale trasferimento costituiva una comunicazione di

dati personali da titolare a titolare per la quale era necessario lo specifico consenso degli interessati, che non risultava acquisito.

Il Tribunale di Treviso, con sentenza n. 3 del 15 febbraio 2011, ha integralmente confermato il provvedimento del Garante.

Sull'impugnazione di una richiesta di informazioni che l'Autorità aveva avanzato, su segnalazione di una nota società di telecomunicazioni, nei confronti di un'associazione per la tutela del diritto d'autore, il Tribunale di Roma ha confermato quanto sostenuto dal Garante sull'inammissibilità dell'opposizione, attesa la natura endoprocedimentale di tipo istruttorio, e quindi non autonomamente impugnabile, della richiesta di informazioni (sentenza n. 20400 del 23 settembre 2011).

Una decisione ha avuto a oggetto il trattamento dei dati genetici effettuato da una persona e dal suo legale i quali, al fine di valutare l'eventuale fondatezza di una instauranda azione giudiziale di disconoscimento della paternità, avevano prelevato campioni biologici dell'interessato, senza il suo consenso, sottoponendoli al *test* genetico sulla variabilità individuale. Su reclamo dell'interessato, il Garante con il provvedimento del 27 novembre 2008 (doc. *web* n. 1581365) aveva vietato qualsiasi ulteriore trattamento dei dati personali genetici, perché acquisiti e trattati in violazione dell'art. 90 del Codice e delle autorizzazioni generali emanate dall'Autorità.

Il giudice ha confermato tale provvedimento, statuendo che la normativa applicabile all'epoca dei fatti prevedeva che per il trattamento dei dati genetici i ricorrenti avrebbero dovuto munirsi dell'autorizzazione del Garante e del consenso informato dell'interessato, anche se il trattamento era finalizzato a far valere un diritto in sede giudiziaria (Tribunale di Roma, sentenza n. 3597 del 18 febbraio 2011).

Conformemente all'eccezione avanzata dall'Autorità, il Tribunale ha, altresì, dichiarato inammissibile, per difetto di legittimazione attiva, il ricorso proposto dall'agenzia investigativa che aveva procurato i campioni biologici, la quale non risultava destinataria del provvedimento opposto.

Con sentenza della Corte di Cassazione si è conclusa la vicenda relativa alla legittimità dell'acquisizione tramite consultazione diretta del casellario giudiziale, da parte di un

Consorzio, del certificato penale dell'amministratore di una società che, risultata aggiudicataria provvisoria di un appalto per pubblico incanto bandito dal Consorzio, era stata poi esclusa dalla gara.

La società aveva proposto ricorso avanti al Tribunale di Padova che, con sentenza n. 2254 del 16 settembre 2004, aveva confermato il provvedimento del Garante del 14 novembre 2003, ritenendo che rientrasse negli obblighi dell'ente appaltante il controllo sulla veridicità delle autocertificazioni prodotte dalle società partecipanti all'appalto, con il potere, a tal fine, di consultazione diretta degli archivi del casellario.

La Corte ha ritenuto corretto e immune da vizi il percorso logico seguito dal giudice del merito, in quanto la pertinente normativa primaria e secondaria equipara la consultazione diretta del casellario da parte di una pubblica amministrazione, quale è il Consorzio, alla consultazione del certificato rilasciato dal casellario stesso (sentenza n. 19364 del 18 luglio 2011).

Infine, come già riportato (*supra*, par. 16.2.), si sono avute due pronunce in materia di giurisdizione.

In entrambi i casi, sia le Sezioni unite della Corte di Cassazione, sia, in altra vicenda, il Tribunale amministrativo regionale del Lazio hanno fatto applicazione dell'art. 152, comma 1, del Codice, che prevede che tutte le controversie che riguardano comunque l'applicazione delle disposizioni del Codice sono attribuite all'autorità giudiziaria ordinaria (Cass., S.u., sentenza n. 8487 del 6 luglio 2010; Tar Lazio, sentenza n. 10161 del 13 dicembre 2011).

16.5. 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 esso possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni–, l'Autorità ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente sue pronunce, 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 tenerla comunque informata sullo svolgimento delle vicende processuali e di riceverne comunicazione in merito agli esiti.

17. L'ATTIVITÀ ISPETTIVA E LE SANZIONI

17.1. LA PROGRAMMAZIONE DELL'ATTIVITÀ ISPETTIVA

L'attività ispettiva, è lo strumento per accertare *in loco* specifiche situazioni di fatto che devono essere oggetto di valutazione da parte dell'Autorità. Essa però è spesso utilizzata anche per acquisire maggiore conoscenza di fenomeni nuovi in vista di una successiva regolazione da parte del Garante attraverso i cd. "provvedimenti generali".

Le ispezioni effettuate nell'anno 2011 sono state 447, sulla base di programmi ispettivi semestrali disposti dall'Autorità.

Come evidenziato anche nelle precedenti Relazioni, l'attività di controllo è stata essenzialmente volta a verificare il rispetto dei principali adempimenti previsti dal Codice da parte di:

- enti pubblici o aziende che gestiscono banche dati di particolare rilevanza o dimensioni, in cui vengono trattati dati di ampie categorie di interessati (ad es., anagrafe tributaria, enti previdenziali, banche, società che gestiscono i pagamenti attraverso carte di credito, fornitori di servizi di telecomunicazioni, 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 particolari tecnologie (ad es., trattamento di dati biometrici, sistemi di rilevazione satellitare, tecnologie di *cloud computing*);
- 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 e a comportamenti illeciti o fraudolenti).

Le linee di indirizzo dell'attività ispettiva sono stabilite dal collegio attraverso delibere di programmazione semestrali che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire.

Sulla base di tali criteri, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche attraverso il sito dell'Autorità (www.garanteprivacy.it, v. *newsletter* n. 345 del 4 febbraio 2011 e n. 349 dell'8 agosto 2011).

Nel 2011, il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva fosse indirizzata a trattamenti di dati personali:

- effettuati da società che gestiscono i pagamenti attraverso carte di credito;
- effettuati da enti previdenziali mediante i propri sistemi informativi;
- in relazione alla formazione e commercializzazione di banche dati per finalità di *marketing* effettuato anche attraverso l'invio di sms, mms ed e-mail;
- effettuati da società che forniscono servizi informatici in modalità *cloud computing*, *hosting*, *housing* e *facility management*;
- effettuati da investigatori privati per lo svolgimento delle investigazioni difensive e per far valere o difendere un diritto in sede giudiziaria.

Nel secondo semestre, invece, oltre alla prosecuzione dei controlli relativi al terzo ed al quarto dei punti ora indicati, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di trattamenti di dati:

- effettuati da società che adottano sistemi che rendono difficile l'individuazione del mittente per l'invio massivo di fax;
- per attività di customer care, effettuati da operatori economici mediante trasferimento di dati all'estero;
- per finalità promozionali, effettuati da società attraverso *call center* e alla verifica del rispetto del diritto di opposizione degli interessati esercitato mediante iscrizione al Registro pubblico di cui all'art. 130, comma 3-*bis*, del Codice;
- effettuati da società di recupero crediti nella fase stragiudiziale, con particolare riferimento ai flussi di dati con soggetti terzi coinvolti nell'attività e alla verifica del rispetto delle prescrizioni impartite dall'Autorità con il provvedimento generale del 30 novembre 2005 [doc. *web* n. 1213644].

Più in generale, nel periodo di riferimento sono state anche 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 con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nonché alla durata della conservazione dei dati nei confronti di soggetti, 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.

17.2. LA COLLABORAZIONE CON LA GUARDIA DI FINANZA

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo, in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto nel dettaglio riferito nelle precedenti Relazioni (cfr., da ultimo, Relazione 2009, p. 240 ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha direttamente effettuato la gran parte degli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti dal Corpo, sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge.

Laddove emergano violazioni penali o amministrative, la Guardia di finanza provvede direttamente a informare l'autorità giudiziaria competente e a formalizzare la contestazione delle sanzioni amministrative accertate.

In tal modo l'Autorità dispone di un dispositivo di controllo flessibile ed articolato che integra l'attività svolta direttamente dal dipartimento ispettivo dell'Autorità e che consente tempestive ed efficaci verifiche sul territorio.

Particolare attenzione è stata rivolta alla formazione del personale incaricato dell'attività ispettiva.

Oltre agli ordinari corsi presso la Scuola di polizia tributaria, denominati "Collaborazione della Guardia di finanza con l'Autorità Garante per la protezione dei dati personali", diretti a illustrare al personale operante nei reparti territoriali del Corpo i princìpi del Codice e le prassi operative nei controlli in materia di *privacy*, è stato anche realizzato un innovativo corso per il personale del Nucleo addetto alle ispezioni e i funzionari dell'Autorità, denominato "*Data Protection Enforcement* - attività di controllo delle banche dati".

Tale attività formativa si colloca nell'ambito delle azioni di accrescimento dell'efficacia dei controlli effettuati sia dal personale del Garante sia da quello della Guardia di finanza, anche sulla scorta di quanto previsto dal protocollo d'intesa tra la Guardia di finanza e l'Autorità.

In tale contesto si è sentita l'esigenza di accrescere le conoscenze di natura tecnico-informatica, per acquisire metodologie utili per l'effettuazione degli accessi alle banche dati, così da individuare in modo più accurato eventuali violazioni.

L'iniziativa, preceduta da un'articolata fase di progettazione, si è sviluppata su tre distinti moduli, il primo dei quali curato dal Servizio informatica del Comando generale della Guardia di finanza, il secondo affidato ad una società di formazione specializzata nel settore e l'ultimo, di natura teorico-pratica, curato da personale dell'Ufficio in possesso di peculiari competenze.

L'attività, che ha riguardato complessivamente 32 persone (di cui 24 militari del Nucleo speciale *privacy* e 8 funzionari dell'Autorità), ha avuto un riscontro ampiamente positivo da parte di tutti i frequentatori e ha comportato un significativo miglioramento della qualità e delle modalità di redazione delle risultanze documentali, che consentirà una migliore valutazione dei fenomeni oggetto delle attività istruttorie.

17.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2011 le ispezioni hanno riguardato:

- 50 controlli nei confronti di ospedali pubblici e cliniche private, con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza;

- 40 controlli nei confronti di fornitori di energia elettrica e gas, con riferimento all'utilizzo dei dati dei clienti;
- 40 controlli nei confronti di società che organizzano eventi e gestiscono parchi giochi, con riferimento al trattamento dei dati dei clienti e all'utilizzo di sistemi di videosorveglianza;
- 40 controlli nei confronti di investigatori privati, con riferimento al rispetto del Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive;
- 30 controlli nei confronti di società che forniscono beni e servizi via internet (*e-commerce*), con riferimento all'utilizzo dei dati dei clienti, anche per finalità di *marketing*;
- 22 controlli nei confronti di società che effettuano l'attivazione di schede telefoniche (*dealer*) per conto di società telefoniche, con riferimento alla liceità dell'utilizzo dei dati dei clienti per l'intestazione delle schede stesse;
- 20 controlli nei confronti di società che gestiscono scuole per il rilascio di patenti nautiche, con riferimento all'utilizzo dei dati dei clienti;
- 15 controlli nei confronti di centri per l'impiego, con riferimento all'utilizzo dei dati delle persone che usufruiscono dei loro servizi, con particolare riferimento all'adozione delle misure di sicurezza;
- 9 controlli nei confronti di società che commercializzano via internet coupon per l'acquisto di beni e servizi offerti da terzi, con riferimento all'acquisizione del consenso degli interessati e all'utilizzo dei dati dei clienti per finalità di *marketing*;
- 8 controlli nei confronti di società che commercializzano banche dati per finalità di *marketing* effettuato anche attraverso l'invio di sms, mms ed e-mail, volti a verificare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati;
- 6 controlli nei confronti di grandi catene alberghiere, autonoleggi e *tour operator* relativamente alle modalità di utilizzo dei pagamenti dei clienti attraverso carte di credito;
- 5 controlli nei confronti di società e/o enti che utilizzano sistemi di localizzazione satellitare, per verificare il rispetto del provvedimento generale adottato in materia dal Garante (provv. 4 ottobre 2011 [doc. *web* n. 1850581]);

- 5 controlli nei confronti di società telefoniche, con riferimento alla profilazione dei clienti per verificare il rispetto delle misure e accorgimenti prescritti dal Garante in sede di verifica preliminare, nonché il rispetto del provvedimento generale "Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione" (provv. 5 giugno 2009 [doc. *web* n. 1629107]);
- 4 controlli nei confronti di società di riscossione crediti, con riferimento alla liceità della raccolta dei dati dei soggetti nei cui riguardi svolgono la propria attività;
- 3 società che gestiscono giochi e scommesse, con riferimento all'utilizzo per finalità di *marketing* dei dati delle ricevitorie;
- 2 controlli nei confronti di compagnie di assicurazione, con riferimento all'utilizzo dei dati dei clienti per finalità di *marketing*;
- 2 controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria", per verificare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di enti previdenziali, volti a verificare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di società che forniscono servizi informatici in modalità *cloud computing*, *hosting*, *housing* e *facility management*.

A questi si aggiungono 142 controlli effettuati nei confronti anche di altre categorie di soggetti, per esigenze istruttorie connesse a specifiche segnalazioni pervenute all'Autorità.

In relazione a quanto emerso dagli accertamenti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

Tra i più rilevanti, in ordine cronologico, si segnalano:

- il provvedimento con il quale il Garante ha vietato il trattamento di dati personali posto in essere da alcune società in relazione all'invio di fax promozionali, senza che fosse rilasciata l'informativa ai sensi dell'art. 13 del Codice e che risultasse la prova del consenso preventivo, specifico e informato degli interessati, ai sensi degli artt. 23 e 130 del Codice (provv. 2 marzo 2011 [doc. *web* n. 1802423]);

- il provvedimento con il quale il Garante ha disposto la cessazione dell'efficacia di un precedente divieto (adottato il 24 febbraio 2010) nei confronti di una società che opera nel settore manifatturiero, con riferimento ai trattamenti di dati dei dipendenti in occasione del loro allontanamento temporaneo dalla postazione di lavoro (provv. 31 marzo 2011 [doc. *web* n. 1807758]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati di persone disabili utilizzati per l'invio di comunicazioni promozionali, in assenza del consenso specifico ed informato degli interessati, ai sensi degli artt. 13, 23 e 26 del Codice (provv. 31 marzo 2011 [doc. *web* n. 1810166]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società tramite la costituzione e diffusione *online* di un elenco telefonico i cui dati non sono stati tratti dal *database* telefonico unico (DBU), utilizzato anche per la funzione di "ricerca inversa", in violazione del provvedimento 15 luglio 2004 (provv. 7 aprile 2011 [doc. *web* n. 1810351]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società che, sebbene conservasse all'estero i dati personali e li gestisse in modalità remota, utilizzava in modo prevalente un apparato di rete (fax *gateway*) collocato sul territorio italiano per l'invio di comunicazioni promozionali senza il consenso degli interessati (provv. 7 aprile 2011 [doc. *web* n. 1810207]);
- i provvedimenti con i quali il Garante ha disposto il blocco dei trattamenti di dati posti in essere con sistemi di videosorveglianza, attraverso i quali era possibile effettuare un controllo a distanza dell'attività lavorativa dei dipendenti, senza l'accordo con le rappresentanze sindacali aziendali né in alternativa, la specifica autorizzazione da parte della direzione provinciale del lavoro (provv. 14 aprile 2011 [doc. *web* n. 1810223], provv. 10 novembre 2011 [doc. *web* n. 1859539], provv. 17 novembre 2011 [doc. *web* nn. 1859558 e 1859546].
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società che inviava fax, e-mail ed sms con modalità automatizzate per conto di terzi rappresentati, nella maggior parte dei casi, *tour operator* che promuovevano "pacchetti vacanze" nei confronti di agenzie di viaggio (provv. 5 maggio 2011 [doc. *web* n. 1822815]);

- il provvedimento generale con il quale il Garante ha impartito al settore bancario prescrizioni in materia di circolazione delle informazioni e di tracciamento delle operazioni di accesso ai dati dei clienti (provv. 12 maggio 2011 [doc. *web* n. 1813953]);
- i provvedimenti con i quali il Garante ha vietato il trattamento dei dati posto in essere da società che comunicavano ad altri soggetti dati per l'invio di comunicazioni commerciali via sms, senza aver rilasciato agli interessati un'idonea informativa ai sensi dell'art. 13 del Codice e senza aver acquisito uno specifico consenso ai sensi dell'art. 23 del Codice stesso (provv. 10 giugno 2011 [doc. *web* n. 1836396]; provv. 26 ottobre 2011 [doc. *web* n. 1851750]);
- il provvedimento con il quale il Garante ha vietato il trattamento dei dati posto in essere da una società, senza aver fornito agli interessati un'idonea informativa ai sensi dell'art. 13 comma 4, del Codice e senza aver acquisito uno specifico consenso per l'invio, via sms, di comunicazioni promozionali automatizzate ai sensi dell'art. 130; i dati erano anche trasferiti all'estero in assenza di uno dei presupposti previsti dagli artt. 43 o 44 del Codice e, quindi, in violazione dell'art. 45 del Codice stesso (provv. 30 giugno 2011 [doc. *web* n. 1834208]);
- il provvedimento con il quale il Garante ha: dichiarato illeciti i trattamenti effettuati da una società in violazione degli artt. 113 e 114 del Codice nonché 4 e 8, l. n. 300/1970, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2, del Codice stesso; vietato la conservazione e la categorizzazione, su base individuale, dei dati personali riferiti alla navigazione internet dei dipendenti, nonché la conservazione dei dati relativi alle utenze telefoniche chiamate dai singoli dipendenti (provv. 21 luglio 2011 [doc. *web* n. 1829641]);
- il provvedimento con il quale il Garante ha vietato il trattamento posto in essere da un'università *online* dei dati (luogo e data di nascita, codice fiscale, cittadinanza) acquisiti mediante il form di registrazione al proprio sito, eccedenti rispetto alla dichiarata finalità del servizio di registrazione –di mantenimento dei contatti con gli utenti interessati al mondo dell'Ateneo e di informazione dei medesimi riguardo alle novità e agli appuntamenti dell'Ateneo stesso– in violazione dei princìpi di pertinenza e non eccedenza di cui all'art. 11 comma 1, lettera *d*) (provv. 7 settembre 2011 [doc. *web* n. 1844176] già cit. al par. 8.3.);

– il provvedimento con il quale il Garante ha accertato la effettiva titolarità del trattamento dei dati di una società fornitrice di servizi telefonici così detti "a valore aggiunto" (VAS), con riguardo alle operazioni di trattamento effettuate nei confronti di diversi operatori telefonici (provv. 15 settembre 2011 [doc. *web* n. 1849872]);

In molti dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha informato il destinatario dell'atto del successivo avvio del procedimento sanzionatorio.

In questi casi, quindi, successivamente alla notifica del provvedimento è stata formalizzata la contestazione delle violazioni nei confronti del soggetto individuato come responsabile.

17.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

17.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

A seguito delle ispezioni effettuate e, più in generale, dall'esame degli atti delle istruttorie svolte dall'Autorità, sono stati rilevati gli estremi per l'invio all'autorità giudiziaria di 37 informative (di cui 16 direttamente da parte dell'Autorità e 21 da parte della Guardia di finanza).

Le segnalazioni relative a presunte violazioni penali hanno riguardato:

– in 20 casi la mancata adozione delle misure minime di sicurezza;
– in 1 caso l'inosservanza di un provvedimento del Garante;
– in 2 casi la falsità nelle dichiarazioni e notificazioni al Garante;
– in 4 casi il trattamento illecito dei dati;
– in 10 casi violazioni della l. n. 300/1970 (Statuto dei lavoratori), punite come reato dall'art. 171 del Codice, o altre violazioni penali previste da disposizioni non contenute nel Codice in materia di protezione dei dati personali.

La violazione penale più segnalata riguarda, anche per l'anno 2011, il mancato rispetto delle disposizioni concernenti le misure minime di sicurezza che chi tratta dati personali (titolari, responsabili ed incaricati) deve adottare per assicurare il livello di sicurezza predefinito dalle norme. Tra queste può essere annoverata anche la designazione degli incaricati del trattamento, che non costituisce un mero adempimento formale, in quanto la

parte più significativa delle misure di sicurezza è strettamente correlata all'attività degli incaricati stessi (ovvero di coloro che ordinariamente operano sui dati personali, cfr. regole 1-10 (autenticazione informatica), 12-15 (adozione di un sistema di autorizzazione), 22 e 23 (dati sensibili contenuti in supporti rimovibili), 27 (dati comuni contenuti in supporti cartacei), 28 e 29 (dati sensibili contenuti in supporti cartacei) dell'Allegato B. al Codice) e mira a fornire loro istruzioni per il corretto trattamento dei dati, rendendoli al contempo consapevoli delle connesse responsabilità anche attraverso specifici processi formativi.

Tale adempimento assume peraltro maggiore significato alla luce dell'orientamento espresso della Corte di Cassazione Sezioni unite penali nella sentenza n. 4694/2012, con riferimento al reato di accesso abusivo a un sistema informatico o telematico, previsto dall'art. 615-*ter* del codice penale.

Secondo la Corte, infatti, *"integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso".*

Seguendo questo principio, si può ritenere che la delimitazione dell'ambito del trattamento consentito all'incaricato e la predisposizione di opportune prescrizioni (istruzioni all'incaricato nella terminologia corrente del Codice) possano costituire la linea di demarcazione rispetto a comportamenti che potrebbero quindi, in tale prospettiva, essere suscettibili di valutazione sotto il profilo penale.

Sotto il profilo procedurale, nel caso in cui venga rilevata l'omessa adozione di una o più misure minime di sicurezza (specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza Allegato B. al Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della relativa violazione e, verificata la regolarizzazione, ammette il responsabile stesso al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazione in ordine all'estinzione del reato.

Con riferimento a questa complessa procedura, i procedimenti definiti nell'anno 2011 connessi al cd. "ravvedimento operoso" in materia di misure minime di sicurezza, sono stati 12 e hanno determinato il pagamento all'Autorità di 432.500 euro da parte delle persone responsabili delle violazioni.

17.4.2. Sanzioni amministrative

A seguito delle ispezioni effettuate e delle istruttorie curate dall'Ufficio, sono stati avviati 358 procedimenti sanzionatori amministrativi.

Le sanzioni amministrative contestate hanno riguardato le seguenti violazioni:

- omessa o inidonea informativa (192);
- trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (100);
- omessa informazione o esibizione al Garante (22);
- violazione del diritto di opposizione (21);
- omessa o incompleta notificazione (11);
- inosservanza di un provvedimento del Garante (11);
- più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza e dimensioni (1).

I procedimenti sanzionatori definiti nell'anno sono stati 281 di cui 202 hanno comportato l'applicazione di una sanzione e 79 sono stati archiviati in quanto la parte ha potuto dimostrare di non aver commesso la violazione contestata o che la violazione non le era imputabile.

Come evidenziano i dati, il maggior numero di sanzioni irrogate ha riguardato la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali, nonché la violazione dell'obbligo di acquisirne il consenso, spesso connessa a trattamenti illeciti per attività di *marketing*.

Per la prima volta sono state anche contestate le violazioni del diritto di opposizione all'utilizzo del proprio numero di telefono per finalità di *marketing*, manifestata attraverso l'iscrizione al Registro pubblico delle opposizioni (fattispecie introdotta all'art. 162, comma

2-*quater*, del Codice con il d.l. 25 settembre 2009, n. 135, convertito dalla l. 20 novembre 2009, n. 166). In tutti i casi nei quali, a seguito di segnalazioni degli interessati, è stato possibile accertare l'effettuazione di chiamate promozionali nei confronti di numerazioni iscritte al registro delle opposizioni, si è proceduto a contestare la violazione del predetto diritto, che prevede una pena pecuniaria da 10.000 a 120.000 euro.

Numerosissime sono le istruttorie già avviate in questo settore ed ancora in corso, sicché nell'anno 2012 il numero di sanzioni per violazione del diritto di opposizione appare destinato ad aumentare notevolmente.

Complessivamente, le entrate relative all'attività sanzionatoria per l'anno 2011 sono state pari a 3.073.430 euro, in relazione a:

- procedimenti sanzionatori spontaneamente definiti mediante pagamento da parte dei contravventori (per un importo di 1.810.400 euro);
- ordinanze-ingiunzione adottate dall'Autorità a seguito dell'esame delle memorie difensive e delle audizioni delle parti (per un importo di 830.530 euro);
- ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (per un importo di 432.500 euro).

I proventi delle sanzioni applicate dal Garante sono devoluti allo Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e sono utilizzati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

17.4.3. Alcuni princìpi rilevabili dalle ordinanze-ingiunzioni adottate dal Garante

Dall'esame delle ordinanze-ingiunzioni adottate dal Garante e pubblicate sul sito è possibile desumere alcuni princìpi di carattere generale.

In un'ordinanza-ingiunzione emessa nei confronti di un'impresa che aveva effettuato un trattamento di dati biometrici per la rilevazione delle presenze dei propri dipendenti senza, tra l'altro, aver richiesto una verifica preliminare (art. 17 del Codice) e senza aver adottato le prescrizioni di cui al provvedimento del Garante "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" del 23 novembre 2006 [doc. *web* n. 1364099], si è posto il problema dell'eventuale congiunta applicabilità della sanzione prevista dall'art. 162, comma 2-*bis*, del Codice per inosservanza del citato art. 17 e di quella di cui all'art. 162, comma 2-*ter*, del Codice stesso per inosservanza di tale provvedimento.

Sulla base degli atti, l'Autorità ha rilevato l'insussistenza di "elementi per applicare la sanzione di cui all'art. 162, comma 2-*ter*", del Codice; in quanto l'utilizzo di un sistema di rilevazione delle presenze basato sul trattamento di dati biometrici dei dipendenti, in un'ipotesi non contemplata dal suddetto provvedimento del 2006, comportava la necessità di richiedere una verifica preliminare ai sensi del citato art. 17, per la cui omissione veniva applicata la sanzione prevista dall'art. 162, comma 2-*bis*, del Codice stesso.

Rilevante anche il principio affermato nella stessa ordinanza-ingiunzione, relativamente all'obbligo di notificazione al Garante di cui all'art. 37, comma 1, del Codice. L'Autorità ha evidenziato che l'omessa notificazione "sostanzia un illecito omissivo di natura permanente, per il quale il momento della consumazione coincide con la cessazione della condotta (effettuazione della notificazione) ovvero con il momento in cui la violazione viene accertata". Ne consegue che il momento in cui la condotta eventualmente cessa, in quanto il soggetto tenuto alla notificazione ancorché in ritardo vi ha provveduto, coincide con il momento della consumazione dell'illecito cui fare riferimento per individuare la norma sanzionatoria applicabile e il termine di decorrenza della prescrizione (ordinanza-ingiunzione 10 giugno 2011 [doc. *web* n. 1859107]).

In un altro caso è stato affrontato un aspetto procedurale circa il rispetto dei termini dell'istruttoria. Al riguardo occorre evidenziare come le norme che regolano i termini dell'istruttoria preliminare dei procedimenti amministrativi del "reclamo" e della "segnalazione" sono contenute negli artt. 11, comma 1 e 14, comma 2, del regolamento del Garante n. 1/2007. I termini relativi al distinto e autonomo procedimento sanzionatorio amministrativo sono, invece, disciplinati dalla l. n. 689/1981, come peraltro indicato nella Tabella A, del regolamento del Garante n. 2/2007. Nel provvedimento l'Autorità afferma che: "l'istruttoria preliminare del procedimento sanzionatorio è volta all'accertamento della violazione

amministrativa ovvero alla valutazione dei dati acquisiti ed afferenti agli elementi costitutivi, sia soggettivi che oggettivi, dell'infrazione. Sul punto, il costante orientamento della giurisprudenza ha ormai reso pacifico il fatto che l'attività di accertamento dell'illecito amministrativo deve essere intesa come comprensiva del tempo necessario alle valutazioni anzidette (*ex multis*, Cass. civ. Sez. II, 30 maggio 2006, n. 12830), senza, quindi, prevedere alcun termine perentorio" (ordinanza-ingiunzione 16 febbraio 2011, [doc. *web* n. 1855692]).

18. LE RELAZIONI INTERNAZIONALI

18.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Conferenza internazionale delle autorità di protezione dati Città del Messico 2011

La 33ª Conferenza internazionale delle autorità di protezione dei dati si è svolta a Città del Messico il 2 e il 3 novembre 2011 con il titolo *"Privacy: The Global Age"*. Nella sessione dedicata esclusivamente alle autorità di protezione dati sono state approvate tre risoluzioni, riguardanti:

- la protezione dei dati personali nel contesto di eventi naturali di particolare gravità; risoluzione proposta dall'autorità della Nuova Zelanda, che incoraggia una riflessione sulla flessibilità della protezione dei dati in funzione della salvaguardia degli interessi vitali delle persone in caso di disastro naturale;
- il rafforzamento dei meccanismi di cooperazione delle autorità in ambito internazionale a fini di *"enforcement"*; risoluzione proposta dai *Commissioners* di Regno Unito e Canada, che istituisce un gruppo di lavoro all'interno della Conferenza per definire un quadro legale ed i possibili meccanismi di coordinamento tra le autorità anche allo scopo di scambiare le informazioni relative a casi di indagini in corso o potenziali;
- l'uso di un identificatore unico nell'impiego del Protocollo internet versione 6 (IPv6); risoluzione proposta dall'autorità tedesca, che raccomanda di mantenerne l'uso anche con l'introduzione del nuovo protocollo di indirizzi temporanei (*dynamic addresses*), *'by default'*.

La Conferenza è stata principalmente dedicata all'esame delle modalità di tutela effettiva e non burocratica della protezione dei dati personali in un contesto in cui lo sviluppo delle tecnologie, le nuove forme di comunicazione in rete, la proliferazione dei dati, l'uso innovativo delle informazioni, hanno aperto orizzonti finora impensabili e al tempo stesso comportato grandi sfide e rischi per i diritti delle persone. Nella consapevolezza della necessità di un approccio globale ai menzionati problemi, si è discusso, in particolare, della sicurezza delle informazioni e della notifica dei cd. *data breaches*, del *cloud computing*, del diritto all'oblio nel mondo digitale, della ridefinizione del concetto di dato personale in relazione agli scenari aperti dalla rete, della necessità di regole riconosciute a livello internazionale.

Nella *"Closed Session"* le autorità hanno inoltre discusso i rapporti del comitato esecutivo sulle modalità di organizzazione delle conferenze internazionali ed il rapporto del comitato per l'accreditamento, accettando le richieste di partecipazione –in qualità di membri– delle autorità della Bosnia Erzegovina e del Marocco –e quali osservatori– di Giappone, Macao, Perù (quest'ultimo a partire dal prossimo anno) e Corea del Sud (per la quale non è ancora stata provata la sussistenza del requisito di indipendenza dell'autorità).

È stato anche dato il benvenuto all'Uruguay, che si è offerto di organizzare la Conferenza internazionale del 2012.

Spring Conference 2011

La *Spring Conference* del 2011, tenutasi a Bruxelles il 5 aprile, ha adottato una risoluzione che ha evidenziato l'esigenza di un approccio globale alla protezione dei dati personali, più idoneo a configurarla quale diritto fondamentale della persona. La Conferenza si è anche occupata della definizione di una politica europea comune in materia di supervisione nel settore della cooperazione giudiziaria e di polizia, sulla base di un documento predisposto dal Garante europeo per la protezione dei dati, oggetto di ampia discussione e che ha condotto nei mesi successivi alla redazione di un ulteriore e più articolato documento da sottoporre alla *Spring Conference* del 2012 per l'approvazione.

Una specifica sessione è stata dedicata al futuro del *Working Party on Police and Justice* (*Wppj*) alla luce del Trattato di Lisbona e dell'opportunità di garantire un'efficace ripartizione delle competenze fra i soggetti incaricati della supervisione (visto che il Gruppo Art. 29 dell'Ue sarà chiamato necessariamente ad occuparsi delle questioni *ex*-III pilastro). È emersa una netta preferenza per la graduale integrazione nelle attività svolte dal *Wppj* delle materie dell'*ex*-III pilastro, con il sostegno degli attuali presidente e vice-presidente del Gruppo stesso.

La Conferenza ha inoltre accettato le richieste di partecipazione dell'Autorità della Repubblica Moldava e dell'Autorità comune di controllo (ACC) di EUROJUST (senza diritto di voto).

18.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

Il Gruppo Art. 29, mantenendo il suo ruolo di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha contribuito al dibattito sull'attualità della

Direttiva n. 95/46/CE e della Decisione quadro 2008/977/GAI del Consiglio dell'Ue, nonché ai lavori preparatori della revisione di tale normativa, che si sono conclusi con la presentazione, il 25 gennaio 2012, del nuovo "pacchetto di riforma" sul trattamento dei dati personali.

Parere 12/2011 sul concetto di consenso

Tale impegno risulta dal programma di lavoro 2010-2011 (WP 170), del quale si è riferito nella Relazione 2010 (v. p. 211) e sulla cui base sono stati adottati diversi pareri e documenti.

Il parere approvato il 13 luglio 2011 (WP 187), sul tema del consenso dell'interessato, relativo anche all'applicazione degli artt. 7, 8 e 26 della Direttiva n. 95/46/CE, fornisce alla Commissione alcune proposte in vista della revisione della direttiva stessa.

In particolare, è stato suggerito di: chiarire il concetto di "inequivocabilità" del consenso, onde evitare che il "silenzio" possa essere considerato un consenso valido; introdurre espressamente il diritto di "revoca" del consenso; enfatizzare i requisiti del consenso "informato" e "preventivo"; con riferimento ai soggetti incapaci, individuare chiaramente in quali circostanze il consenso possa essere manifestato dai genitori o dal rappresentante legale del soggetto incapace e, nel caso di minori, rendere obbligatorio l'uso di meccanismi di verifica dell'età del soggetto.

Lettera del Gruppo alla Commissione europea del 20 aprile 2011

Il Gruppo ha inoltre adottato alcuni documenti quali *"advice paper"*, per sottoporre alla Commissione europea, senza pretese di esaustività, alcune proposte di modifica della normativa, su tre questioni di particolare interesse: i dati sensibili, la semplificazione degli obblighi di notificazione, la cooperazione tra le autorità di protezione dei dati personali.

I documenti sono accompagnati da una lettera alla Commissione (20 aprile 2011), che indica le soluzioni che hanno ottenuto la maggioranza dei consensi. In particolare, per i dati sensibili, il divieto di trattamento con lista "chiusa", salvo eccezioni. In materia di notificazione, un sistema basato su una "lista positiva" di trattamenti per i quali è necessaria la notificazione, analogamente al modello italiano. In materia di cooperazione, è stato posto l'accento sull'esigenza di maggiore armonizzazione relativamente ai poteri, alle competenze e all'indipendenza delle autorità di protezione dei dati personali.

Nella lettera viene, infine, rappresentata l'opportunità che i *paper* in questione siano letti insieme al parere del Gruppo in materia di revisione della direttiva (WP 168 del 1° dicembre 2009), alla lettera trasmessa dal Gruppo alla Commissaria Reding il 14 gennaio 2011 (*Letter*

from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication 'A comprehensive approach to personal data protection in the EU') e al parere sulla legge applicabile (WP 179 del 16 dicembre 2010), esortando la Commissione a riflettere sulla scelta di soluzioni che evitino il ricorso al *"forum shopping"* in materia di protezione dei dati personali.

Sempre in linea con il programma di lavoro 2010-2011, il Gruppo ha dedicato particolare attenzione alle cd. "sfide tecnologiche" per la protezione dei dati, sia in relazione alla revisione della Direttiva n. 2002/58/CE, operata attraverso le Direttive nn. 2009/136/CE e 2009/140/CE, fornendo chiarimenti interpretativi ed operativi sull'applicazione della norma di nuova introduzione relativa alla "notifica delle violazioni di dati" (art. 4, par. 3 della Direttiva n. 2002/58/CE aggiunto dalla Direttiva n. 2009/136/CE) (WP 184 del 5 aprile 2011) sia commentando il codice di autodisciplina proposto dall'*International Advertising Bureau* (*IAB*), al fine di regolamentare l'utilizzo di *cookies* per tracciare la navigazione degli utenti di internet allo scopo di proporre pubblicità mirata (*targeted advertising*) (WP 188 dell'8 dicembre 2011).

Parere 1/2011 sul quadro regolamentare applicabile ai *data breach*

Nel parere relativo all'obbligo di notifica delle violazioni dei dati (*data breach notification*), il Gruppo ha sottolineato la necessità di armonizzare gli atti nazionali di recepimento (previsti dalla Direttiva entro il 25 maggio 2011), stabilire criteri di notifica dei *data breach*, con particolare riferimento agli aspetti tecnico-operativi (tempi di notifica, soglie di gravità, canali di comunicazione) ed assicurare la coerenza, anche terminologica, tra i provvedimenti normativi previsti per il recepimento delle modifiche della direttiva *e-privacy* e gli atti di trasposizione della Direttiva n. 95/46/CE. Si tratterrà di raccogliere le informazioni ed esperienze nazionali in vista della creazione della "Piattaforma" di lavoro comune menzionata nel documento, anche ai fini della cooperazione con gli altri soggetti competenti per la definizione degli specifici meccanismi attuativi (Agenzia europea per la sicurezza delle reti e dell'informazione-ENISA, Garante europeo della protezione dei dati, Commissione europea).

Parere 16/2011 sulle raccomandazioni EASA/IAB sulla pubblicità comportamentale *online*

Nel parere sulla pubblicità comportamentale e protezione dei dati personali *online* (WP 188 dell'8 dicembre 2011), il Gruppo, concentrandosi sui princìpi del consenso e dell'informativa, precondizioni essenziali alla valutazione della legittimità del trattamento, è giunto

alla conclusione che i meccanismi stabiliti nel codice di autoregolamentazione adottato nell'aprile 2011 dalla *European Advertising Standards Alliance (EASA) e dall'Internet Advertising Bureau Europe* (*IAB*), non sono in linea con il requisito del consenso preventivo (*opt-in*) per l'installazione di *cookies* a fini diversi dalla prestazione del servizio di comunicazione o di un servizio espressamente richiesto dall'utente (art. 5, par. 3, Direttiva n. 2002/58/CE). Tuttavia, vengono segnalate varie possibilità tecniche per l'espressione di tale consenso (fra cui una opportuna configurazione dei parametri di navigazione internet, *"browser settings"*, anche attraverso il suggerimento italiano di appositi dispositivi *"plug-in"* configurabili a seconda dello specifico *browser*, o la creazione di *opt-in cookies*), evidenziando alcuni elementi positivi ma migliorabili (ad esempio l'uso di un'icona per l'informazione iniziale dell'utente, da sviluppare in linea con il principio della *"layered information notice"*, sostenuto dal Gruppo Art. 29 nel proprio parere WP 100).

Inoltre (anche attraverso uno scambio di corrispondenza con IAB) è stata sottolineata la portata non esaustiva degli strumenti di autodisciplina a tutela dei princìpi sanciti nell'art. 5, par. 3 della Direttiva.

Parere 13/2011 sui servizi di geolocalizzazione tramite *smart mobile devices*

Il parere in tema di geolocalizzazione e servizi mobili intelligenti (smartphones) (WP 185 del 16 maggio 2011), è volto a chiarire i profili di responsabilità dei gestori telefonici e dei produttori/distributori di applicazioni (*apps*) per i dispositivi mobili. Questi contengono infatti una vasta gamma di informazioni riservate, anche sensibili, quali i dati relativi alla posta elettronica, alle immagini private, alla cronologia di navigazione internet, alla rubrica telefonica. Sulla base di una dettagliata analisi tecnica, alla quale seguono considerazioni di ordine giuridico rispetto all'applicazione delle Direttive nn. 2002/58/CE e 95/46/CE, il Gruppo raccomanda ai produttori di *software* ed ai fornitori di applicazioni di geolocalizzazione, titolari del trattamento dei dati personali raccolti attraverso tali sistemi, di assicurare informative adeguate, l'esercizio dei diritti degli interessati e la messa a disposizione di strumenti *"user-friendly"* per definire il livello di dettaglio della localizzazione (cosiddetta "granularità" del servizio). Inoltre, pur riconoscendo che in talune circostanze (ad esempio in presenza di aree urbane densamente popolate) l'associazione fra i codici di accesso dei singoli dispositivi (che sono identificatori univoci dell'apparecchio) e i dati di localizzazione non

consente necessariamente di identificare una persona fisica determinata, il Gruppo sottolinea la necessità di considerare le informazioni in oggetto alla stregua di dati personali, a meno che il titolare possa dimostrare in modo ragionevole che i dati raccolti non sono personali.

Nel corso del 2011 sono stati poi adottati il parere relativo ai cd. "contatori intelligenti" (*smart meters*) nel settore delle forniture di gas, elettricità ed altri servizi (WP 183 del 4 aprile 2011) ed il parere sulla nuova proposta di *privacy impact assessment* relativo alle tecnologie *RFID* (WP 180 dell'11 febbraio 2011).

Parere 12/2011 sui "contatori intelligenti"

Il parere sui contatori intelligenti presuppone la definizione di un concetto chiave quale l'*"energy fingerprint"*, che fa riferimento al fatto che le modalità di consumo di energia proprie di ciascun utente, possono, in talune circostanze, costituire un dato identificativo dell'interessato, in analogia a quanto avviene con il concetto di *"browsing fingerprint"* per i servizi della società dell'informazione erogati sulla rete internet. Il Gruppo ha suggerito al riguardo di prevedere specifiche garanzie di protezione dati nell'ambito dei contratti di fornitura di energia, nonché un più ampio ricorso al principio di *"Privacy by Design"* nella progettazione di tali dispositivi. Si è sottolineato che le raccomandazioni formulate, riguardanti anche la responsabilità del trattamento dei dati e la più puntuale individuazione dei fondamenti di legittimità del trattamento, si basano sulle conoscenze attualmente disponibili, e che interventi ulteriori da parte del Gruppo potrebbero rendersi necessari per valutare aspetti di futura emersione (specie rispetto all'attuazione del principio di *"Privacy by Design"*).

Motori di ricerca

Sempre nel contesto delle nuove tecnologie, alla luce dei recenti sviluppi relativi alla nuova *"Privacy Policy"* di *Google*, in particolare, con riferimento alla previsione di un'informativa unica valida per tutti i servizi offerti che presenta aspetti non del tutto chiari quanto al possibile raggruppamento anche dei dati personali raccolti per tali servizi in un unico *"repository"* centrale, il Gruppo ha chiesto a *Google Inc.* una pausa di riflessione segnalando l'intenzione di ottenere ulteriori delucidazioni in merito (lettera del 2 febbraio 2012). I Garanti hanno inoltre sostenuto l'autorità irlandese nell'attività di audit da essa condotta nei riguardi di *Facebook Ireland ltd.*, la filiale irlandese di *Facebook*, responsabile dei trattamenti di dati personali concernenti cittadini o soggetti stabiliti nell'Ue, i cui sviluppi sono costantemente monitorati in modo congiunto.

In tema di trasferimento di dati verso Paesi terzi, su richiesta della Commissione europea, che dovrà esprimersi con una decisione sul punto, il Gruppo ha adottato un parere favorevole alla valutazione di adeguatezza del livello di protezione offerto dalla Nuova Zelanda (WP 182 del 4 aprile 2011).

Parere 11/2011 sul livello di protezione dei dati personali nella Nuova Zelanda

Il Gruppo ha inoltre continuato ad occuparsi del trasferimento e trattamento dei dati in ambito finanziario.

In particolare, con il parere 14/2011 (WP 186 del 13 giugno 2011), è stato affrontato il tema della tutela dei dati personali nel contesto della prevenzione dei fenomeni del riciclaggio di denaro e del finanziamento del terrorismo e sono state fornite raccomandazioni per i soggetti coinvolti nella regolamentazione e nell'*enforcement* a scopo di prevenzione di tali fenomeni.

Parere 14/2011 sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo

Per quanto riguarda la cooperazione amministrativa internazionale nel settore della vigilanza sulle società di revisione contabile, tra le autorità competenti dell'Ue e quella degli Stati Uniti (*Public Companies Account Oversight Body - PCAOB*), è stata indirizzata alla Commissione europea una lettera-parere (13 dicembre 2011), volta a fornire indicazioni sul rispetto dei requisiti di protezione dei dati personali nel contesto della cooperazione amministrativa, ai sensi della Direttiva n. 2006/43/CE (cd. ottava direttiva) sul controllo della revisione dei conti, anche al fine di valutare gli accordi per la protezione dei dati personali ("data protection arrangements") tra le autorità di vigilanza del settore.

Lettera del 13 dicembre 2011 sui trasferimenti internazionali di dati allo *US Public Accounting Oversight Body - PCAOB*

È stato poi portato all'attenzione del Gruppo il tema della compatibilità della legge degli Stati Uniti, denominata *"Foreign Account Tax Compliance Act - FATCA"*, che entrerà in vigore il 1° gennaio 2013, con la legislazione di protezione dati europea. Obiettivo della *FATCA* è il contrasto all'evasione fiscale "offshore" (incluso il territorio dell'Unione europea) ad opera di *"US persons"* che abbiano effettuato investimenti in Europa. La Commissione europea ha chiesto al Gruppo Art. 29 di formulare una lettera/parere sulle criticità poste dai trattamenti di dati personali conseguenti all'applicazione della legislazione *FATCA*, in particolare con riferimento alla base giuridica, alla legittimità del trattamento, alla tipologia dei dati personali richiesti, ai soggetti coinvolti e alla possibilità di *"onward transfer"*, ossia di ulteriori trasferimenti dei dati. Il problema è in corso di esame da parte del Gruppo, anche alla luce dei possibili futuri accordi in materia tra Stati Uniti e Stati membri dell'Unione europea.

Binding corporate rules - BCR

In materia di *binding corporate rules* (*BCR*) il lavoro si è concentrato sulla definizione di un nuovo modello di *BCR*, chiamato *"BCR for data processor"*, ispirato alle *"BCR for controller"*, che dovrebbe consentire i trasferimenti transfrontalieri di dati all'interno di una società multinazionale di servizi. Il sistema è concepito secondo un doppio schema: il cliente (titolare) sottoscrive un contratto generale di servizi (*Service Level Agreement - SLA*) con la società multinazionale (responsabile); tra le clausole contrattuali sono ricomprese le *"BCR for processor"* (allegate allo *SLA*) tramite le quali la società multinazionale ha la possibilità di "sub-appaltare" le attività di trattamento (o alcune fasi di esso) alle proprie consociate, anche stabilite in Paesi terzi, senza necessità di ulteriori formalità (autorizzazioni *ad hoc*, *standard contractual clauses*, ecc.). Lo schema di *"BCR for processor"* ricalca quello delle *"BCR for controller"* nei suoi princìpi fondamentali: efficacia vincolante delle *BCR*, clausola del terzo beneficiario a favore dell'interessato; clausola di responsabilità con attrazione della giurisdizione nell'Unione europea; rispetto dei princìpi della Direttiva n. 95/46/CE; impegno per il gruppo multinazionale a dotarsi di un sistema di *training*, a disporre di una struttura specializzata nella gestione delle segnalazioni degli interessate a svolgere audit periodici sul rispetto dei princìpi di protezione dati.

Nell'ambito dell'attività volta a semplificare gli oneri a carico delle imprese interessate, è stata discussa l'opportunità di elaborare dei modelli base di *"audit"* e *"training"*. Gli schemi sono attualmente in corso di perfezionamento e saranno verosimilmente resi pubblici nel corso del 2012.

"Terrorist Finance Tracking Program", cd. TFTP2

Il Gruppo ha inoltre proseguito la discussione sul monitoraggio dell'attuazione dell'accordo sulla trasmissione dei dati di messaggistica finanziaria tra Unione europea e Stati Uniti (*"Terrorist Finance Tracking Program"*, cd. *TFTP2*), che ha visto, tra l'altro, il controllo da parte di EUROPOL delle richieste di trasferimento di dati finanziari dall'Unione europea al Dipartimento del Tesoro degli Stati Uniti.

È stato oggetto di approfondito esame, in particolare, il rapporto relativo alla revisione congiunta, svoltasi a Washington il 17 e 18 febbraio 2011 (*"Commission report on the joint review of the implementation of the Agreement"*). Il rapporto è stato formulato dal team per l'Unione europea (composto anche dalle autorità del Belgio e dei Paesi Bassi) e sottoposto, per integrazioni, al team degli Stati Uniti.

Sempre sull'attuazione dell'accordo *TFTP2*, si segnala il rapporto sull'ispezione effettuata dall'Autorità di controllo comune (ACC) EUROPOL (su cui, v. anche par. 18.3. e Relazione 2010, p. 229). Al riguardo si osserva che i compiti aggiuntivi attribuiti ad EUROPOL in virtù dell'accordo *TFTP* tra l'Unione europea e gli Stati Uniti determinano una correlativa espansione della competenza dell'Autorità di controllo comune, al fine di verificare la legittimità anche dei trattamenti di dati personali effettuati ai sensi di tale accordo.

Nella lettera del 7 giugno 2011 al Dipartimento del Tesoro degli Stati Uniti sull'interpretazione dell'accordo *TFTP2*, il Gruppo pone il problema di come garantire l'effettivo esercizio del diritto d'accesso degli interessati ai dati oggetto di trattamento in base all'accordo, e delle modalità da seguire, in particolare, per quanto concerne l'accertamento dell'identità del richiedente. È stato infatti stato rilevato che le richieste di accesso, trasmesse al Dipartimento del Tesoro degli Stati Uniti, possono essere ritenute inammissibili se non sufficientemente dettagliate e comunque non conformi alle regole procedurali stabilite dallo stesso Dipartimento. Nella lettera si esprime, tra l'altro, l'intento di raggiungere un *common understanding* con gli Stati Uniti sull'applicazione dell'accordo *TFTP2*.

Sistema europeo per il tracciamento delle transazioni finanziarie a scopo di antiterrorismo - *EU TFTP*

Il Gruppo Art. 29 è stato anche consultato sull'istituendo sistema europeo per il tracciamento delle transazioni finanziarie a scopo di antiterrorismo (cd. *EU TFTP*, basato sulla raccolta e l'analisi dei dati di messaggistica finanziaria). Al riguardo, in relazione alla Comunicazione della Commissione europea [COM(2011) 429] sul programma di monitoraggio delle transazioni finanziarie *EU TFTP*, con lettera del 22 settembre 2011 alla Commissaria Malmström, è stata sottolineata la vaghezza del contenuto della Comunicazione stessa in merito alla futura architettura e alle funzioni del sistema informativo e sono state segnalate sia la possibile sovrapposizione con altri strumenti esistenti intesi a perseguire il medesimo obiettivo, sia le criticità derivanti dall'adozione di un sistema *TFTP* del tutto nuovo, da utilizzare come strumento europeo per finalità di contrasto del terrorismo.

Parere 10/2011 sul sistema di *PNR* europeo

Il parere del Gruppo sulla proposta di direttiva della Commissione europea, che istituisce un sistema europeo di utilizzo dei dati del codice di prenotazione (*PNR*) ai fini di prevenzione, accertamento, indagine ed esercizio dell'azione penale nei confronti dei reati di terrorismo e di altri reati gravi (WP 181 del 5 aprile 2011), ha analizzato principalmente la

necessità e la proporzionalità del sistema oltre che le modalità di trattamento previste. Riprendendo argomentazioni già formulate nel parere adottato congiuntamente con il *Wppj* sul precedente testo (lettera-parere del 18 dicembre 2007), non si sono ritenute sufficientemente dimostrate né la necessità del sistema, né la sua utilità specifica rispetto all'obbligo per le stesse compagnie di fornire in anticipo i dati *API* (*Advance Passenger Information*) dei passeggeri. Quanto alla proporzionalità, perplessità si esprimono in particolare sui rischi di una raccolta indiscriminata di dati a prescindere da reali esigenze legate alla commissione di reati, sulla notevole ampiezza del campo di applicazione e del margine di manovra lasciato agli Stati membri, sulla lunghezza del periodo e sulle modalità di conservazione dei dati, sul vasto numero di dati richiesti, inclusi quelli sensibili, nonché sul ruolo e le responsabilità delle *"Passenger Information Unit"* (*PIU*) nel trattamento dei dati.

Si segnala, infine, che il Gruppo si è espresso anche in merito agli accordi *PNR* con Stati Uniti/Canada/Australia, con lettera del 19 gennaio 2011, inviata alla Commissaria responsabile per gli Affari interni della Commissione europea, Cecilia Malmström. Nel testo si sottolineano i punti critici già evidenziati nei precedenti interventi del Gruppo (v. Relazione 2010, p. 222) ovvero: in primo luogo la non dimostrata necessità di ricorrere ai dati *PNR* per le finalità di cui agli accordi; i tempi di conservazione dei dati da parte delle autorità di *law enforcement*; i presupposti e le modalità per il trasferimento dei dati e per l'accesso agli stessi; il trasferimento ulteriore dei dati (*onward transfer*) ad altre autorità e/o Stati terzi; il controllo, la durata e la revisione congiunta degli accordi.

Parere 1/2012 su epSOS

Per quanto concerne i dati sanitari, il Gruppo si è occupato del progetto epSOS (*Smart Open Services for European Patients*) in materia di protezione dei dati personali, per l'interoperabilità nel settore della sanità elettronica, co-finanziato dalla Commissione europea, al quale partecipano 47 soggetti (tra cui ministeri della salute e aziende private) in rappresentanza di 20 Stati membri (e di 3 Stati extra-Ue: Svizzera, Turchia e Norvegia). L'obiettivo principale è la creazione di un sistema di *e-health* (comprensivo della relativa infrastruttura di *Information Technology-IT*) che consenta di accedere, in maniera sicura e nel rispetto della *privacy*, alle informazioni sanitarie dei pazienti. L'interscambio di dati avviene mediante una rete informatica composta da *National Contact Point– "NCP"* (circa

uno per ogni partecipante) i quali svolgono il ruolo di interfaccia nazionale nei confronti dei *Point of Care - "POC"* (medici, strutture sanitarie, farmacie, veicoli di emergenza, ecc.) situati nello Stato membro estero e aderenti al progetto epSOS. Il *NCP* è considerato il principale referente del funzionamento del progetto, poiché ha competenza a contrarre con gli organismi sul territorio ed ha il compito di curare il rispetto delle regole in materia di sicurezza e riservatezza dei dati trasferiti.

Nel parere del Gruppo (WP 189 del 25 gennaio 2012), particolare attenzione è stata rivolta all'esigenza di individuare esattamente il titolare ed il responsabile del trattamento, nonché eventuali forme di contitolarità dello stesso. Inoltre, sono state fornite indicazioni relativamente alle modalità di acquisizione del consenso (affinché si specifichi quando esso riguardi la partecipazione al progetto e quando, invece, sia rivolto al singolo trattamento sanitario richiesto), all'informativa (che dovrà indicare in maniera chiara le caratteristiche tecniche del trasferimento di dati all'interno del sistema) e alle misure di sicurezza (che dovranno garantire un elevato livello di protezione dei dati nell'ambito dell'intero processo di interscambio degli stessi).

Infine, quanto agli aspetti problematici legati al sempre maggiore uso della biometria nell'ambito delle nuove tecnologie (ad esempio, la diffusione delle tecniche di riconoscimento facciale, vocale, ecc.), il Gruppo sta predisponendo un nuovo parere generale, ed uno più specifico relativo al riconoscimento facciale, che dovrebbe essere approvato nel corso del 2012.

È stato altresì riattivato il sottogruppo *WADA* (*World Anti-Doping Agency*), che, in occasione della revisione del codice mondiale antidoping, fornirà indicazioni alla Commissione europea sulla protezione dei dati personali nel contesto della lotta al doping nelle attività sportive professionali.

18.3. LA COOPERAZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Working Party on Police and Justice (Wppj)

Nel 2011 il *Wppj* ha proseguito, sotto la presidenza italiana, le attività avviate in base al "Programma di lavoro" approvato nel 2009, ed ha condotto un'approfondita riflessione sul proprio ruolo e sulle modalità utili a garantire un migliore coordinamento con il Gruppo

Art. 29, alla luce dell'unificazione del quadro normativo di protezione dati, prevista dal Trattato di Lisbona, sia pure con i contemperamenti indicati nelle dichiarazioni ad esso allegate.

Al riguardo, le riunioni tenutesi presso la sede del Consiglio Ue a Bruxelles e l'intenso scambio di documentazione fra le delegazioni, hanno permesso di delineare un possibile quadro di competenze e collaborazione, anche sulla base delle richieste, formulate al *Wppj* in occasione della *Spring Conference* 2011, di valutare quali delle sue competenze potessero essere trasferite al Gruppo Art. 29, rispetto alle tematiche *ex*-III Pilastro ricadenti prevalentemente o esclusivamente nell'ambito dell'Ue. Sulla base di tali premesse, il *Wppj* ha stabilito di completare le attività già in corso e programmate aventi rilevanza paneuropea: analisi delle problematiche connesse allo scambio e trattamento di dati Dna fra autorità giudiziarie e di polizia a livello europeo, anche con riguardo all'utilizzo dei canali INTERPOL; individuazione degli ambiti di una possibile indagine coordinata paneuropea sulla base del metodo di analisi del rischio delineato nel "Catalogo" sviluppato dal *Wppj* in tema di cooperazione e supervisione (approvato dalla *Spring Conference* del 2009); potenziamento della cooperazione con il Consiglio d'Europa rispetto alla revisione della Convenzione n. 108/1981 e della Raccomandazione n. R(87)15 sul trattamento dei dati per fini di polizia. Peraltro, il *Wppj* ha stabilito di trasferire al Gruppo Art. 29 ogni competenza in merito alla valutazione dello stato di attuazione della decisione-quadro sulla protezione dei dati personali nell'*ex*-III Pilastro (decisione quadro 2008/977/GAI del Consiglio dell'Ue), ricadendo quest'ultima in un ambito esclusivamente legato all'Ue.

Relativamente all'indagine sul trattamento e scambio di dati Dna in ambito giudiziario e di polizia, le risposte al questionario circolato nel corso del 2010 e nei primi mesi del 2011, pur in presenza di un quadro parziale, hanno evidenziato numerose difformità a livello nazionale, anche con riguardo alle misure di sicurezza in essere. Il *Wppj* ha quindi iniziato ad elaborare possibili indicazioni operative omogenee, anche alla luce di esperienze sviluppate in altri ambiti internazionali (in particolare, INTERPOL).

L'analisi condotta in base ai criteri delineati nel "Catalogo" ha portato ad individuare nei trattamenti di dati relativi a soggetti non sospettati di reati (conoscenti e/o contatti personali di sospetti e/o criminali) un'area di particolare delicatezza per quanto riguarda le attività di

polizia e giudiziarie, tenuto conto della sensibilità delle informazioni potenzialmente raccolte e dell'assenza o dell'opacità di disposizioni normative sul punto. Il *Wppj* ha quindi elaborato, in via provvisoria, una lista di quesiti e tematiche sulle quali chiedere specifiche delucidazioni attraverso un'eventuale indagine paneuropea.

Il *Wppj* ha seguito attentamente il dibattito in seno ai competenti gruppi di lavoro del Consiglio d'Europa (Comitato consultivo cd. *T-PD*) con riguardo sia alla revisione (modernizzazione) della Convenzione n. 108/1981 sia all'analisi della Raccomandazione R(87)15; molte delegazioni del *Wppj* avevano già fornito indicazioni attraverso il questionario che il Consiglio aveva fatto circolare fra le autorità nazionali competenti, nel corso del 2011, per valutare lo stato di attuazione della Raccomandazione e le relative problematiche (v. *infra*).

Nei prossimi mesi le attività sopra descritte dovranno trovare compiuta conclusione e le autorità europee di protezione dati (riunite nella *Spring Conference* 2012) dovranno pronunciarsi sul futuro del *Wppj*. Resta indubbio il contributo fornito da quest'ultimo nel monitorare possibili criticità nel settore della cooperazione giudiziaria e di polizia in materia penale, indicando anche soluzioni o strumenti armonizzati utili a garantire la salvaguardia dei diritti riconosciuti ai cittadini europei.

Riunioni congiunte delle autorità di controllo comune (ACC) EUROPOL, EUROJUST, Schengen, Dogane

Dell'incontro congiunto delle autorità di controllo comune EUROPOL, EUROJUST, Schengen e Dogane svoltosi il 1 febbraio 2011 si è riferito nella Relazione 2010 (p. 229).

Si è svolta a Bruxelles, nei giorni 1° e 2 marzo 2011, la successiva riunione delle ACC, nella quale è stato deciso di concentrare l'analisi programmatica, già iniziata nella riunione di Lubiana, sugli elementi necessari per una buona supervisione, senza bloccarsi su questioni nominalistiche.

EUROPOL: l'attività dell'Autorità di controllo comune (ACC) e del comitato ricorsi

Una riunione straordinaria dell'ACC EUROPOL si è tenuta il 31 gennaio 2011 a Lubiana per approvare il rapporto dell'ispezione svolta presso EUROPOL da un ristretto gruppo di esperti per acquisire informazioni sull'attività svolta nel quadro dell'accordo *TFTP2* Ue-Stati Uniti. Il documento è stato redatto con classifica di sicurezza "Segreto Ue" e non è pertanto accessibile nemmeno agli stessi componenti dell'ACC. Per esigenze di trasparenza è stato redatto un comunicato dando atto delle operazioni compiute e descrivendo gli elementi che possono essere resi pubblici (v. anche par. 18.2. e Relazione 2010, p. 229).

Grande attenzione è stata riservata dal Parlamento europeo al rapporto presentato sull'ispezione ed è stata evidenziata la questione dell'accesso ai documenti dell'ACC.

L'Acc EUROPOL ha poi svolto una seconda ispezione, a distanza di un anno dalla precedente, per verificare lo stato di attuazione delle prescrizioni impartite e lo stato del trattamento dei dati. Anche questo secondo rapporto, una volta approvato dall'ACC, sarà soggetto alle stesse regole di segretezza e sarà comunque redatto un comunicato pubblico sui risultati.

Anche mediante incontri con i responsabili di EUROPOL, è stata analizzata la proposta di far confluire gli attuali archivi di analisi in due contenitori più ampi, dedicati rispettivamente al terrorismo ed al crimine organizzato. In particolare, il 4 maggio 2011, presso la sede di EUROPOL a l'Aja, si è tenuto l'incontro tra i responsabili di EUROPOL, il segretariato comune delle ACC e i componenti del sottogruppo *Analytical Work File* (*AWF*) dell'ACC EUROPOL, per ottenere le informazioni necessarie per comprendere le ragioni della proposta e valutare come essa possa essere considerata in linea con le previsioni della Decisione EUROPOL (Decisione 2009/371/GAI del Consiglio dell'Ue).

Conseguentemente, EUROPOL ha evidenziato la compatibilità della proposta con il quadro legale esistente, con riferimento all'architettura dei nuovi *AWF*, (archivi di lavoro per fini di analisi), ai compiti e alle responsabilità, alle modalità di accesso e alle misure di sicurezza. Nei successivi incontri volti a definire le valutazioni dell'Autorità in merito, sono state espresse perplessità in relazione ai dati ricevuti e non ancora attribuiti ad una specifica analisi, per quanto attiene al rispetto del principio di finalità. L'ACC dopo lunga discussione, ha informato con una lettera il direttore di EUROPOL che *prima facie* non ritiene tale modo di operare in contrasto con il quadro legale esistente e che non intende bloccare i lavori, anche se è indispensabile chiarire molti aspetti non secondari, per non abbassare il livello di garanzie e le possibilità di controllo oggi esistenti.

Sono state inoltre discusse le prime risultanze della 13ª ispezione annuale svoltasi nel marzo 2011 presso l'EUROPOL, e, in particolare, i punti critici emersi, in relazione sia alla perdurante mancata attuazione di alcune raccomandazioni formulate nelle precedenti ispezioni, sia alle risultanze dei controlli effettuati, che hanno riguardato sei file di analisi, incluso quello relativo al *TFTP*, il sistema di informazione EUROPOL (EIS), l'accesso di

EUROPOL al SIS, il sistema di messaggistica SIENA, il sistema di analisi EUROPOL (EAS), nonché i dati relativi ai dipendenti.

Al termine della discussione si è deciso, come prassi, di inviare copia della bozza di rapporto, senza le raccomandazioni, ad EUROPOL, che ha potuto formulare eventuali commenti poi valutati nel corso della successiva riunione, il 28 settembre, quando è stato adottato il rapporto di ispezione con le relative raccomandazioni.

Si è anche discusso della possibilità di verificare le condizioni e le modalità di accesso delle unità nazionali ed è stato suggerito di sviluppare una metodologia comune e di redigere una *checklist* affinché le Autorità di protezione dei dati possano svolgere in maniera efficace le loro attività di supervisione e controllo.

Il Comitato ricorsi di EUROPOL si è invece occupato di due ricorsi, ritenendo per il primo di dover ulteriormente consultare EUROPOL. Per il secondo, è stata invece adottata una bozza di decisione, che rileva come EUROPOL non abbia rispettato il disposto dell'art. 19 della Decisione EUROPOL, non avendo provato che nella specifica ipotesi l'accesso alle informazioni da parte del richiedente avrebbe rischiato di compromettere l'attività della stessa EUROPOL.

Il Sistema informativo Schengen (SIS): attività dell'ACC

In occasione della riunione dell'ACC Schengen nei giorni 1° e 2 marzo 2011, è stato approvato il testo del questionario da inviare alle autorità nazionali competenti, come prima parte dell'azione comune da svolgere per verificare la legittimità delle segnalazioni inserite nel SIS in base all'art. 95 (mandato di arresto europeo) della Convenzione Schengen. Sono stati inoltre definiti i tempi per lo svolgimento della stessa azione comune, in modo che il rapporto finale dell'ACC possa essere redatto con le raccomandazioni eventualmente necessarie. L'attività è cominciata nel giugno 2011 ed è tuttora in corso. Se ne prevede il completamento entro il primo trimestre del 2012.

Rispetto alle precedenti verifiche, l'attività da un lato è risultata più onerosa, in quanto è stato richiesto di ispezionare un campione di segnalazioni fissato in relazione al numero complessivo di segnalazioni inserite da ciascun Paese (per l'Italia circa 200), ma dall'altro lato è stata facilitata dal fatto che fosse prevista una sola fonte di inserimento, il *SIRENE* (*Supplementary Information Request at the National Entry*, la banca dati che raccoglie le informazioni aggiuntive utili a dare seguito alle segnalazioni inserite nel SIS).

Nel frattempo è stata richiesta anche una verifica del seguito dato alle raccomandazioni contenute nel rapporto relativo alle segnalazioni di cui all'art. 99 della suddetta Convenzione.

Si registrano altresì progressi per quanto riguarda la preparazione dell'ispezione al sistema centrale C-SIS a Strasburgo.

Il Sistema informativo doganale (SID): *CIS Supervision Coordination Group* e ACC Dogane

Nella riunione del 1° e 2 marzo 2011, l'ACC Dogane ha organizzato un'ispezione al sistema centrale del Sistema informativo doganale (SID), da svolgersi con l'ausilio del Garante europeo della protezione dei dati (EDPS), a causa delle complicate basi giuridiche. L'ispezione ha avuto luogo il 12 e 13 ottobre 2011, il rapporto inviato in bozza all'Ufficio europeo per la lotta antifrode (OLAF) per commenti, è in via di adozione. L'attività ispettiva conferma che il sistema è poco usato (poco più di 200 file) e che tuttavia vi sono dati eccedenti quelli consentiti dalla base giuridica.

Nell'ambito della riunione dell'ACC Dogane è stato discusso un memo preparato dal segretariato, relativo all'impatto sulle competenze dell'ACC, della decisione quadro sulla protezione dei dati personali nell'*ex*-III Pilastro (Decisione quadro 2008/977/GAI).

Con i rappresentanti dell'EDPS, sono poi stati trattati i punti relativi all'organizzazione dell'ispezione del SID ed al manuale per l'utilizzo del FIDE (Archivio di identificazione dei fascicoli a fini doganali), tuttora in preparazione.

Quanto a quest'ultimo, si è previsto che i segretariati dell'ACC e dell'EDPS lavorino alla redazione di una *checklist*. È stata quindi preparata una bozza di parere congiunto che solleva, rispetto alla versione del manuale del 2009, questioni relative a: la possibilità di usare il FIDE come archivio nazionale, le modalità di accesso al SID per i pubblici ministeri, la possibilità di replicare l'archivio SID in quelli nazionali, i periodi di conservazione dei dati nel sistema.

Per quanto riguarda la riunione del CIS *Supervision Coordination Group* (Gruppo di coordinamento della supervisione del SID), il rappresentante dell'OLAF ha svolto un'interessante presentazione sul funzionamento del sistema FIDE e del relativo manuale, che però contiene un modello di tutela dei dati non soddisfacente. Inoltre, è stato rilevato che l'attuale base giuridica risulta troppo complicata, ed è allo studio un intervento normativo. Al riguardo, si registrano diverse ipotesi, che spaziano dal consolidamento del Regolamento

(CE) n. 515/97 del 13 marzo 1997 ed emendamento della Decisione 2009/917/GAI del 3 novembre 2009 (in particolare, la cancellazione dell'ACC Dogane e l'attribuzione delle competenze all'EDPS con poteri di coordinamento secondo il modello CIS) alla modificazione del solo regolamento, ovvero ancora al rinvio alla Direzione generale affari interni della Commissione europea della parte *ex*-III Pilastro del SID, che quindi non rientrerebbe più nelle competenze di OLAF.

È stato altresì discusso il programma di azione, da definire tendendo conto anche delle attività da svolgere in cooperazione con l'ACC Dogane.

18.4. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Case Handling Workshop

Il 23° incontro del *"Case Handling Workshop"*, svoltosi a Varsavia il 4 e 5 ottobre 2011, è stato suddiviso in sessioni plenarie e sessioni parallele (la cui composizione ha tenuto conto delle dimensioni delle autorità) nelle quali sono stati discussi alcuni *case studies* relativi agli argomenti presentati in plenaria.

Il *workshop* in apertura è stato dedicato ai complessi temi della legge applicabile e della cooperazione tra le autorità in relazione ai casi transfrontalieri. Le differenze tra i poteri attribuiti a ciascuna autorità nell'ambito del proprio ordinamento e l'obbligatorietà o meno della risposta su casi singoli sono stati considerati tra i principali ostacoli di ordine "normativo" alla cooperazione. A ciò si aggiungono ostacoli di natura pratica, quali, ad esempio, la lingua da usare per la cooperazione e la fruibilità, per un'altra autorità, delle prove raccolte in lingua straniera.

Condivisa è stata l'esigenza di una struttura che possa occuparsi delle traduzioni attribuendo alle stesse un canone di ufficialità, che ne consenta l'utilizzo nei diversi Paesi europei, nonché di disporre di una lista aggiornata di punti di contatto all'interno delle singole autorità per facilitare la cooperazione.

Il *workshop* si è anche occupato del trattamento di dati *online*, sui *social network* e attraverso il *cloud computing*. Si è convenuto sulla necessità di adottare un *privacy impact assessment* (valutazione dell'impatto-*privacy*) che consenta di valutare i rischi derivanti dall'uso di tali sistemi ed individuare meglio le forme di tutela utili; sulla designazione come

responsabile del trattamento del soggetto che offre il servizio di *cloud* e sulla esigenza di rispettare le disposizioni in materia di trasferimento dei dati all'estero nel caso in cui i dati vengano trattati presso *server* situati fuori dal territorio dell'Unione europea.

È stato discusso in tale ambito anche il caso della Municipalità di Odense, in Danimarca, che, nel febbraio 2010, ha chiesto all'autorità di protezione dati un parere circa l'utilizzo del sistema *"Google apps"* da parte degli insegnanti per l'archiviazione e il trattamento di dati (anche sensibili) relativi ad alunni e genitori. La necessità di rispettare le disposizioni in materia di trasferimento dei dati all'estero (visto che *Google Ireland Ltd.* ha rappresentato di raccogliere i dati su *server* collocati anche negli Stati Uniti) e di adottare più compiute istruzioni da impartire al responsabile del trattamento e maggiori misure di sicurezza (ad es., ottenendo maggiori dettagli in ordine sia alle modalità di distruzione dei dati in caso di risoluzione del contratto, sia ai sistemi di *"logging"* per verificare eventuali accessi illeciti) sono stati i principali aspetti su cui si è soffermata l'autorità.

La terza sessione dei lavori ha consentito, tanto nella fase plenaria, con le presentazioni da parte dell'EDPS e delle Autorità della Svizzera, della Francia e della Polonia, quanto nell'ambito dei sottogruppi, di confrontare le diverse modalità ispettive adottate dalle autorità di protezione dei dati. Interessante è stata reputata, compatibilmente con le potenzialità dell'organico, la possibilità di verificare, a distanza di tempo, l'adeguamento del titolare del trattamento alle misure indicate dalle autorità a seguito di una prima ispezione.

Nel sottogruppo, l'autorità del Regno Unito (*Information Commissioner's Office-ICO*) ha presentato il proprio sistema di audit, illustrando brevemente le linee-guida adottate in materia nel mese di maggio 2011 e citando quale esempio la relazione dell'audit consensuale effettuato con *Google Inc.*, dopo l'illecita raccolta di dati effettuata nell'ambito di *Google Street View*. A seguito dell'audit (la cui relazione –come le altre– è disponibile sul sito dell'*ICO*), l'Autorità ha evidenziato alcuni aspetti positivi delle politiche di *privacy* della società e individuato alcuni punti da potenziare, come l'informativa agli utenti dei differenti servizi.

La sessione dedicata al trattamento dei dati personali in ambito lavorativo (tema che continua a interessare tutte le autorità alla luce dei numerosi casi da affrontare), ha consentito di illustrare alcuni casi recenti in materia di trattamento di dati biometrici (soprattutto

impronte digitali) sui luoghi di lavoro. Unanime la valutazione sulla difficoltà di utilizzare il consenso quale presupposto di legittimità del trattamento dei dati in tale contesto, alla luce della dubbia libertà del lavoratore nel rifiutarlo.

IWGDPT: Il "Gruppo di Berlino" - *International Working Group on Data Protection in Telecommunication (IWGDPT)*

Nel 2011, come di consueto, il "Gruppo di Berlino" si è riunito due volte: la prima a Montreal (4 e 5 aprile); la seconda a Berlino (12 e 13 settembre).

Per quanto riguarda la riunione di Montreal, si segnala l'adozione del paper *"Event Data Recorders (EDR) on Vehicles - Privacy and data protection issues for governments and manufacturers"*. Questo documento prende in esame i "registratori di dati evento" (dispositivi installati su alcune autovetture per registrare informazioni in caso di incidenti e in grado di memorizzare il verificarsi di avarie al motore o improvvisi cambiamenti della velocità delle ruote), tenendo conto della possibilità che essi consentono la periodica trasmissione delle informazioni registrate sul veicolo ad un soggetto esterno. Poiché tale registrazione comporta il trattamento di dati personali relativi al guidatore o ai passeggeri (es. velocità sostenuta, utilizzo o meno di cinture di sicurezza) che potrebbero essere trattati per diverse finalità (gestione dei sinistri da parte delle compagnie di assicurazione, offerta di servizi di emergenza, attività di *marketing*, repressione dei reati), il Gruppo, nell'auspicare al più presto un intervento normativo, ha fornito alcune preliminari raccomandazioni in materia di trasparenza, consenso dell'interessato, modalità del trattamento e misure di sicurezza.

I temi affrontati nella riunione di Berlino hanno spaziato dall'analisi delle implicazioni per la *privacy* derivanti dall'adozione del protocollo internet IPv.6, alle raccomandazioni rivolte ai gestori ed utilizzatori di sistemi come *e-Call* (dispositivi per la sicurezza degli autoveicoli), al *cloud computing*, all'accordo commerciale Ue-Stati Uniti in materia di lotta alla contraffazione e tutela della proprietà intellettuale, anche *online* (*Anti-Counterfeiting Trade Agreement*), fino alle indicazioni fornite alle competenti autorità in materia di micropagamenti effettuati *online* (in particolare tramite smartphones).

A proposito dell'utilizzo del protocollo IPv6, è stato evidenziato che la migrazione dall'attuale protocollo (IPv4) non sarà rapida e che è prevedibile un lungo periodo di coesistenza tra i due protocolli. Pur non essendo possibile esprimere un parere definitivo sulle implicazioni *privacy* del protocollo, che presenta aspetti favorevoli per gli utenti, derivanti

dall'abbondanza di indirizzi (come la possibilità di molteplici allocazioni di indirizzi per singola sessione), e svantaggi non trascurabili, quali la possibilità di dedicare porzioni degli indirizzi a dati ad elevato potere identificativo (quali gli indirizzi MAC dei terminali e dati di localizzazione), il Gruppo ha auspicato un'applicazione quanto più possibile uniforme su scala globale del protocollo IPv6 e dei meccanismi di conversione IPv4-IPv6.

Relativamente al tema del *cloud computing*, il Gruppo ha individuato nella *"loss of control"* (perdita di controllo) da parte del titolare, il principale problema per l'introduzione su larga scala di questo nuovo servizio. Al fine di restituire al titolare un maggiore potere di controllo sul *provider*, il Gruppo ha auspicato l'introduzione, come strumento immediato di intervento, di meccanismi di *"location audit"* che consentano l'accertamento –da parte del titolare– sia della localizzazione dei *server* in cui sono conservati i dati, sia della *"applicable law"*, con particolare riferimento ai soggetti che possono avere accesso ai dati. Sull'argomento, i rappresentanti del Garante hanno illustrato l'avanzamento di nuove tecniche crittografiche (*Homomorphic Encryption*) in grado di consentire trattamenti direttamente su dati cifrati, senza che il *provider* sia a conoscenza dei dati trattati, che potrebbero innalzare il livello di fiducia sull'impiego dei servizi di *cloud computing*.

Il Gruppo ha inoltre raccomandato ai governi nazionali e alle autorità competenti di consentire l'effettuazione di micropagamenti elettronici in forma anonima, ovvero attraverso l'impiego di pseudonimi, onde evitare forme occulte di tracciamento legate ai beni o servizi acquistati tramite tali modalità di pagamento (spesso per somme minime o assai contenute); essenziale anche la previsione di adeguate informative per gli utenti, che illustrino i rischi associati a tali modalità.

Le riunioni hanno permesso di rappresentare novità o sviluppi nazionali di possibile interesse comune. In particolare, i rappresentanti del Garante hanno illustrato il provvedimento sull'invio di fax originati da apparecchi situati al di fuori del territorio nazionale [doc. *web* n. 1810207] ed i punti principali della campagna informativa sul tema *cloud computing* (documento annesso alla relazione annuale 2010), prima iniziativa di *"awareness raising"* rivolta alle imprese intrapresa da un'autorità di protezione dati. È stato illustrato anche il documento del Garante sul diritto all'oblio e sull'applicazione a tale scopo del protocollo

"robots.txt". Il documento ha ricevuto un riscontro positivo da parte del Gruppo di Berlino, che ha deciso di mantenerne l'impianto generale con alcune modifiche proposte dall'assemblea, sottoponendolo al consueto processo di valutazione e approvazione congiunta in vista di una sua definitiva approvazione nel corso del 2012.

"Data Retention - Expert Group"

Nell'ambito dei lavori dell'*Expert Group "The Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime"*, la Commissione europea ha illustrato il report sulla valutazione della Direttiva 2006/24, annunciando l'intenzione di presentare una proposta di revisione della direttiva entro la fine dell'anno. A tal fine, sono stati istituiti, tre sottogruppi sugli aspetti più critici, in relazione alla protezione dei dati personali, all'attività delle forze di polizia, all'impatto competitivo della direttiva ed alle politiche di rimborso dei costi da parte degli Stati membri. Infine, il sottogruppo *"Data Preservation"* fornirà indicazioni sull'impiego dello strumento del *"quick freeze"*, volte a chiarire anche se questo sia da considerare sostitutivo o complementare rispetto alla *"data retention"*.

La Commissione europea, visto il ruolo di coordinamento svolto dal Garante nell'azione congiunta di *enforcement* del Gruppo di lavoro Art. 29, ha chiesto all'autorità di protezione dati italiana di fare da *rapporteur* per il sottogruppo *"Data Protection"*.

Sono emerse visioni molto contrastanti sia sull'attuazione della direttiva sia sulle proposte di modifica. La complessità dei lavori non ha consentito di rispettare il termine sopra indicato.

Secondo la Commissione europea comunque è fondamentale una maggiore armonizzazione delle regole a livello dell'Unione, da ottenere tramite la definizione di un periodo unico di conservazione; l'armonizzazione del concetto di *"serious crime"*; l'individuazione delle *LEA* (*law enforcement agencies*) autorizzate all'accesso ai dati.

L'*"accountability"*

Si è aperta la fase conclusiva del processo di approfondimento iniziato nel 2009 con il *"Galway Project"*, volto all'individuazione degli elementi fondamentali della *accountability* (responsabilità, sul cui concetto v. anche Relazione 2010, pp. 214 e 218) e seguito, nel 2010 dal *"Paris Project"* (II fase), nel 2011 dal *"Madrid Project"* (III fase) e nel 2012 dal *"Brussels Project"* (IV fase attuale). Il progetto ha portato alla formulazione di un primo documento riepilogativo dei criteri che dimostrano e misurano il livello di *accountability* dei titolari del

trattamento (*"Demonstrating and Measuring Accountability - A Discussion Document"*). Partendo dalle affermazioni di principio contenute nel predetto documento, il progetto si è poi concentrato sull'individuazione di soluzioni pratiche e condivise su quanto sarà richiesto alle società di parte dei cd. *"agenti di accountability"* (*validators*), sul come e quando le società potranno certificare la propria accountability, nonché sugli incentivi che i regolatori potranno fornire alle società per incoraggiarle e conseguire livelli sempre più alti di accountability, previa una valutazione dei rischi di *privacy* e dei danni che le società stesse possono creare quando trattano dati personali in mancanza di accountability.

I lavori seguono in parallelo quelli dell'OCSE dedicati alla rielaborazione delle linee-guida del 1980.

Consiglio d'Europa

Nel 2011 l'Autorità ha proseguito la sua partecipazione ai lavori del Comitato consultivo (*T-Pd*) della Convenzione n. 108/1981 del Consiglio d'Europa (CoE), prevalentemente dedicata alla modernizzazione della Convenzione stessa.

Nella 27ª riunione plenaria (dal 29 novembre al 2 dicembre 2011), la discussione si è concentrata sul documento predisposto dal Segretariato, recante alcune proposte di modifica del testo attuale.

Da un punto di vista più generale, in seguito a un dibattito che ha coinvolto l'Ufficio Trattati della Direzione generale dei diritti umani e stato di diritto del CoE, è risultato non ancora chiaro l'impatto –in termini di rilevanza della Convenzione n. 108/1981– della futura adesione dell'Unione europea alla Convenzione europea dei diritti dell'uomo (CEDU).

Al riguardo, il segretariato del Consiglio d'Europa ha escluso, al momento, che la Convenzione n. 108/1981, quale documento di ausilio per l'interpretazione dell'art. 8 della Convenzione europea dei diritti dell'uomo, possa rappresentare (in caso di adesione dell'Ue alla CEDU) un parametro di legalità degli atti comunitari. Il segretariato ha preferito insistere sul carattere internazionale della Convenzione n. 108/1981, tale da vincolare Stati extra-Ue all'adozione di legislazioni conformi.

Per quanto riguarda il testo delle modifiche proposte, in relazione ai flussi transfrontalieri di dati, si è evidenziata l'importanza di assicurare la compatibilità degli obblighi giuridici derivanti dalla Convenzione con quelli previsti dalla normativa comunitaria (per evitare, ad

es. che uno Stato sia considerato "adeguato" ai sensi della Convenzione, ma non ai sensi della Direttiva n. 95/46/CE). È stata sottolineata, altresì, la necessità di meccanismi di verifica della "adeguatezza" (degli Stati, ma anche delle norme contrattuali d'impresa).

Con riferimento alle definizioni è prevalso l'orientamento di valorizzare il carattere "generale" della Convenzione, evitando definizioni eccessivamente dettagliate.

Sempre in questa prospettiva di semplificazione, nonché di estensione dell'ambito di applicazione della Convenzione, si è proposto di fare riferimento alla nozione di *"data processing"* piuttosto che a quella di "file".

È stata ben accolta da quasi tutte le delegazioni l'introduzione di una categoria "aperta" di dati sensibili, che si caratterizzerebbe in relazione a seri rischi di un pregiudizio all'integrità fisica dell'interessato o di discriminazioni arbitrarie e illegittime nei suoi confronti.

Si è concordato sull'opportunità di riferire l'adeguatezza delle misure di sicurezza al rischio del trattamento e alla natura dei dati trattati, tenendo altresì conto delle dimensioni del titolare (grande o piccola e media impresa) e del numero dei soggetti potenzialmente lesi dalle *security breaches* (violazioni della sicurezza).

In linea generale, le delegazioni hanno espresso parere positivo sull'introduzione dei princìpi di accountability, ("responsabilità"), *privacy by design* e *privacy impact assessment* (valutazione dell'impatto *privacy*).

Nel 2012 le delegazioni saranno invitate a prendere posizione sulla nuova versione della Convenzione.

OCSE - WPISP

In ambito OCSE, il *Working Party on Information Security and Privacy* (*WPISP*), nel 2011 ha focalizzato la sua attività in modo particolare sulla revisione delle linee-guida OCSE del 1980 sulla protezione della *privacy*.

Si ricorda che, a seguito degli eventi organizzati nel 2010 in occasione del trentennale delle citate linee-guida (v. Relazione 2010, p. 240), l'OCSE ha reso pubblico il rapporto *"The Evolving Privacy Landscape"*, nel quale vengono identificati i punti di forza e le criticità delle linee-guida stesse anche in vista della loro revisione.

Il processo di revisione è stato avviato con il coinvolgimento delle diverse delegazioni partecipanti all'OCSE, compresi i rappresentanti del mondo dell'industria e della società

civile, chiamati a fornire il proprio punto di vista attraverso una consultazione pubblica, conclusasi il 1° aprile 2011. Dalla consultazione è emerso un primo quadro di riferimento sulle sfide per la *privacy* rappresentate dalle nuove tecnologie e dalla globalizzazione, sono stati individuati alcuni princìpi chiave che potrebbero essere introdotti nel processo di rielaborazione delle linee-guida e delineate le modalità di lavoro che saranno seguite nell'attività di revisione.

A margine della Conferenza internazionale di Città del Messico, l'OCSE ha organizzato un incontro sulla revisione delle linee-guida, dando conto anche del processo di modernizzazione in corso in sede Ue e nell'ambito del Consiglio d'Europa e sullo sviluppo della regolamentazione in materia di *privacy* in America latina.

Quanto alle possibili modifiche delle linee-guida, il VG (*Volunteer Group of Privacy Experts*) del *WPISP*, nella riunione del 30 novembre 2011, ha in primo luogo discusso sull'opportunità di formulare una raccomandazione per la revisione dei soli "princìpi base" (contenuti nella Parte 2 delle linee-guida) o, viceversa, per la revisione anche delle altre parti (ad es., la Parte 3, relativa ai trasferimenti internazionali di dati). È stato inoltre proposto di aggiungere una parte relativa al nuovo ruolo assunto dall'interessato nel mutato quadro tecnologico rispetto al trattamento di dati personali e di prevedere la traduzione del citato rapporto esplicativo in una seconda lingua.

Quanto al tema del valore economico dei dati personali, già oggetto della Tavola rotonda del dicembre 2010 organizzata dal *WPISP* e dal *WPIE* (*Working Party on the Information Economy*), sempre in occasione del 30° anniversario delle linee-guida, è stata sottolineata l'esigenza di proseguire la collaborazione *WPISP/WPIE*, in particolare, concentrandosi sulla crescita del business legato alla protezione dei dati ed analizzando il rapporto tra costi e benefici nella tutela della *privacy*.

Il *Directorate for Employment, Labour and Social Affairs - Health Committee* dell'OCSE ha predisposto un rapporto (datato 9 novembre 2011) sull'uso secondario dei dati sanitari a scopi di ricerca e di implementazione delle politiche sanitarie pubbliche, che mette in evidenza gli aspetti più problematici dell'applicazione dei princìpi *privacy* nel settore della sanità. Il *WPISP*, in merito, ha sottolineato che la protezione dei dati non costituisce un

ostacolo allo sviluppo di politiche sanitarie e della ricerca in tale ambito, e che occorre, invece, individuare un corretto bilanciamento dei diversi interessi in gioco, nel dovuto rispetto dei diritti delle persone.

A fronte del considerevole incremento dell'uso di internet su dispositivi mobili da parte dei minori e del notevole aumento di reati commessi a loro danno attraverso i *social network* e la telefonia mobile, il *WPISP* ha elaborato un rapporto (datato 2 maggio 2011) sulla protezione dei minori *online*, cui è seguita una Raccomandazione dell'OCSE (16 febbraio 2012).

Tale Raccomandazione è volta a fornire un quadro di princìpi generali sulle *policy* da adottare a tutela dei minori, diretti alle diverse categorie coinvolte (i minori stessi, i genitori, le scuole, i fornitori di servizi, i governi). Il tutto nella consapevolezza che il problema essenziale consiste nella natura aperta di internet e nella esigenza che siano contemporaneamente rispettati alcuni diritti, in particolare la libertà di espressione e il diritto alla *privacy*.

Incontri con delegazioni estere

Dell'incontro svoltosi nel gennaio 2011 nell'ambito del progetto di gemellaggio *"Strengthening Data Protection in Israel"*, si è riferito nella Relazione 2010 (p. 241).

19. Le attività di comunicazione, studio e ricerca

19.1. La comunicazione del Garante: profili generali

Nel 2011, l'attività di comunicazione curata dal Garante si è focalizzata principalmente su alcuni temi rispetto ai quali si è posta l'esigenza di equilibrare interessi in gioco particolarmente rilevanti: il fisco; gli istituti bancari ed il tracciamento delle operazioni; la trasparenza nella pubblica amministrazione; la ricerca medica e la sanità; la tutela dei lavoratori; il mondo della scuola; la mediazione civile; il giornalismo e la tutela dei minori; la giustizia ed il corretto rapporto tra diritto di cronaca e tutela degli indagati; il nuovo regime del *telemarketing*; internet; il *cloud computing* e la protezione dei dati in rete; le grandi banche dati pubbliche e private.

L'Autorità ha, come di consueto, affidato la sua informazione ad un linguaggio semplice e chiaro, mirato ad una funzione divulgativa realmente al servizio dei cittadini, ritenendo che il compito istituzionale sia non solo quello di far rispettare le regole che sono alla base di un corretto uso dei dati e tutelare la riservatezza delle persone, ma anche quello di promuovere e sviluppare la consapevolezza dell'importanza assunta in generale nella società contemporanea della protezione dei dati e del ruolo indispensabile svolto dal Garante.

Nell'era di internet, dell'ICT e delle nuove forme di comunicazione elettronica che offrono enormi opportunità, ma presentano evidenti rischi per la tutela dei dati personali, la vera sfida è quella di riuscire a governare le tecnologie e di tutelare la libertà di chi le utilizza.

Lo sforzo di comunicazione e sensibilizzazione ha avuto un particolare riscontro sugli organi di informazione. L'interesse dei *media* per le tematiche riguardanti la protezione dei dati personali e per le attività del Garante è rimasto stabile rispetto allo scorso anno. Nel periodo dal 1° gennaio al 31 dicembre 2011, il Servizio relazioni con i mezzi di informazione ha selezionato 35.700 articoli di interesse dell'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media online*, che hanno dedicato spazio alle questioni legate generalmente alla *privacy*, sono state circa 10.900, delle quali oltre 3.200 dedicate esclusivamente all'attività del Garante.

19.2. I PRODOTTI INFORMATIVI

Nel corso del 2011 l'Autorità ha diffuso 35 comunicati stampa e 9 *newsletter*.

La *newsletter* periodica, giunta al suo tredicesimo anno di pubblicazione (per un totale di 353 numeri e di 1.230 notizie), è uno strumento di centrale riferimento dell'attività svolta dal Garante. La *newsletter* ha consentito di continuare a far conoscere i provvedimenti di maggior interesse adottati dall'Autorità in campo sia nazionale sia internazionale, nonché un articolato panorama di temi e problematiche. La pubblicazione, oltre a poter essere consultata *online* sul sito *web* del Garante, viene inviata in via telematica ad un numero sempre maggiore di abbonati (istituzioni, privati cittadini, liberi professionisti, imprese).

Nel 2011, è stata pubblicata la ventunesima edizione del Dvd "Il Garante e la protezione dei dati personali". Il Dvd si apre con una presentazione multimediale che, attraverso animazioni e testi, illustra l'attività, le funzioni e l'organizzazione dell'Autorità. L'aggiornato archivio digitale ipertestuale consente una consultazione *full-text* della normativa nazionale ed internazionale, dei provvedimenti adottati dall'Autorità, della raccolta completa dei comunicati stampa e delle *newsletter*. Ogni anno, realizzato in 5.000 copie, il Dvd, oltre ad essere inviato a quanti ne fanno espressa richiesta, viene distribuito in occasione di manifestazioni nazionali, convegni, incontri e seminari ai quali partecipa il Garante.

Il piano di comunicazione istituzionale, attraverso opuscoli e strumenti di divulgazione e destinato ad un vasto pubblico, è proseguito con la pubblicazione di un nuovo *vademecum* dedicato alla sanità intitolato "Dalla parte del paziente. *Privacy*: le domande più frequenti" e di schede di documentazione con raccomandazioni per il corretto e consapevole trattamento dei dati personali, con riferimento all'impiego di nuovi strumenti di comunicazione, come gli smartphone e i tablet, e all'erogazione di servizi informatici che comportano l'esternalizzazione di dati e procedure come il *cloud computing*.

19.3. PRODOTTI EDITORIALI

La collana editoriale "Contributi" –che raccoglie testi di approfondimento sulle problematiche riguardanti la *privacy* e la tutela della dignità della persona– nel corso dell'anno si è arricchita della terza edizione aggiornata del volume "*Privacy* e giornalismo", a cura del componente del Garante Mauro Paissan. Il volume, come una sorta di manuale

pratico, raccoglie le numerose decisioni, i provvedimenti e le prese di posizione del Garante sul delicato equilibrio tra diritto di cronaca e riservatezza dei cittadini. Si tratta di interventi innovativi, al passo con i tempi che impongono nuove sensibilità e nuove risposte: basti pensare alle problematiche connesse al giornalismo *online*, ai videofonini, ad internet e ai *social network*, agli archivi *online* dei quotidiani, per non parlare della tutela dei minori, della pubblicazione integrale di intercettazioni, della diffusione di dati sulla salute e sulla vita sessuale, sia di persone note sia di privati cittadini. "*Privacy* e giornalismo" si è rivelato un utile strumento per i giornalisti e per coloro che vogliono intraprendere la professione.

È stata, infine, pubblicata una prima edizione di tutte le linee-guida adottate in questi anni dal Garante in diversi settori, dalla pubblica amministrazione alla sanità elettronica, dalle banche all'informazione giuridica.

19.4. GLI INCONTRI INTERNAZIONALI

Nel corso del 2011 l'Autorità ha partecipato ad importanti incontri internazionali come indicato più ampiamente nella sezione relativa alle relazioni internazionali (vedi par.18.1.).

Il 2 e il 3 novembre si è svolta a Città del Messico la 33ª Conferenza internazionale delle autorità di protezione dei dati, alla quale ha partecipato il presidente Francesco Pizzetti. Tema cruciale della conferenza, che ha visto riuniti rappresentanti provenienti da tutti i continenti, è stata la protezione dei dati personali in un'era globale. In un'epoca in cui internet e l'ICT hanno abbattuto i confini geografici, le autorità per la protezione dei dati di tutto il mondo si sono trovate di fronte alla necessità di modificare la loro azione, sviluppando soprattutto un approccio globale ai problemi e definendo nuove regole comuni in grado di garantire una effettiva tutela della *privacy* oltre i confini nazionali. Nella due giorni di lavori i garanti si sono confrontati, su questioni rilevanti: la globalizzazione, le grandi banche dati, la profilazione degli individui, i nuovi fenomeni tecnologici come il *cloud computing*, il diritto all'oblio nel mondo digitale. A conclusione della conferenza sono state adottate tre risoluzioni: una sull'uso del nuovo protocollo internet per l'assegnazione degli indirizzi (IPv6); una seconda sulla necessità di un coordinamento rafforzato a livello internazionale; una terza sulla protezione dei dati in caso di disastri ambientali.

Dall'11 al 12 novembre si è svolta a Milano la Conferenza internazionale sul tema "Internet fra libertà e diritti". Il presidente Pizzetti, anche nella veste di coordinatore del gruppo europeo per la cooperazione giudiziaria e di polizia (*Wppj*), ha partecipato all'incontro con un intervento dal titolo "Autoesposizione personale sulla rete. I *social network* tra libertà di comunicazione e rischi per la protezione della *privacy*". L'intervento ha offerto anche l'occasione per ribadire che il Garante continua a seguire con la massima attenzione gli sviluppi delle nuove forme di comunicazione sulla rete, anche a livello europeo ed internazionale, per definire regole e comportamenti che tutelino gli utenti, in modo particolare i più giovani, e le libertà individuali.

19.5. LE MANIFESTAZIONI E LE CONFERENZE

L'attività dell'Autorità collegata a seminari, convegni ed altre iniziative a carattere divulgativo ha visto, anche nel corso del 2011, la conferma di un grande interesse da parte del pubblico. Il Garante ha assicurato la sua presenza ad importanti manifestazioni con il proprio stand e con la partecipazione dei suoi rappresentanti a convegni e dibattiti.

Il 28 gennaio di ogni anno ricorre la "Giornata europea della protezione dei dati personali". L'iniziativa, nata nel 2007, viene celebrata in tutta Europa con il sostegno della Commissione europea e di tutte le Autorità preposte alla protezione dei dati nei Paesi europei. Nel 2011, per celebrare l'evento, il Garante ha voluto coinvolgere gli studenti delle terze e quarte classi delle scuole superiori invitandoli a partecipare al concorso "*Privacy* 2.0 - I giovani e le nuove tecnologie", organizzato in collaborazione con la Guida Monaci. Il concorso prevedeva la realizzazione di un "corto" sulla protezione dei dati personali in rapporto all'uso della rete e delle nuove tecnologie. Per usare in maniera consapevole gli strumenti messi a disposizione dalle nuove tecnologie è necessario conoscerne potenzialità e rischi, perciò il Garante ha voluto che fossero i ragazzi a realizzare, attraverso i loro video e improvvisandosi attori e registi, una campagna di informazione e sensibilizzazione sulla protezione dei dati. L'iniziativa ha riscosso grande interesse tra i giovani e numerosi sono stati i contributi video pervenuti, tutti molto interessanti. Una giuria di esperti ha selezionato i lavori ed individuato i tre migliori video. La premiazione dei finalisti si è svolta il 28 gennaio 2012, in occasione della "Giornata europea

della protezione dei dati personali". Al video vincitore intitolato "Proteggi il tuo mondo" (realizzato dal Liceo "Galileo Ferraris" di Taranto) è andato un premio di 5.000 euro, mentre al secondo e terzo posto si sono classificati i video "Pubblica intimità" (realizzato dal Liceo "Amaldi" di Novi Ligure) e "Una vita inscatolata" (realizzato dall'Istituto Magistrale "Renier" di Belluno), premiati con targhe ricordo. Premiate con targhe e strumenti didattici anche le scuole degli studenti vincitori, per aver sostenuto i ragazzi nell'impegno di confrontarsi con un tema così rilevante nella nostra società, come quello della *privacy*.

Dal 9 al 12 maggio 2011 si è svolta la 22ª edizione del *Forum Pa* –Expo 2011. Il Servizio relazioni con i mezzi di informazione, ha assicurato la consueta presenza del Garante all'importante appuntamento, assolvendo al compito istituzionale di promuovere la conoscenza della legge presso cittadini ed operatori, sia pubblici sia privati. L'intera giornata congressuale dell'11 maggio –organizzata in collaborazione con il Garante– è stata dedicata alla "1ª Conferenza nazionale del *cloud computing* per la p.a.", proprio per fare il punto sullo stato dell'arte, sulle opportunità, sui rischi della tecnologia *cloud* che ha già visto grandi investimenti in molti paesi industrializzati e inizia ad essere utilizzata anche nella pubblica amministrazione italiana. La conferenza è stata presieduta dal presidente Pizzetti, che è intervenuto sul tema "*Cloud Computing*, Sicurezza e *Privacy*".

Sul tema del corretto rapporto fra trasparenza della p.a. e tutela della *privacy* del cittadino, è intervenuto invece il componente del Garante, Giuseppe Fortunato, nell'ambito del convegno "La riforma della p.a e la trasparenza: rendere conto ai cittadini", svoltosi anch'esso l'11 maggio.

Nel corso dei quattro giorni della manifestazione, presso lo stand del Garante, sono stati proiettati due video divulgativi: il primo, contenente una moderna presentazione multimediale dell'attività del Garante; il secondo, appositamente realizzato in occasione della "Giornata europea per la protezione dei dati personali" del 2010, che racconta con l'aiuto del cinema le piccole e grandi "invasioni" nella nostra sfera privata. Il video raccoglie spezzoni e sequenze di diversi film che direttamente o indirettamente affrontano i temi della *privacy*, vista nei suoi aspetti più quotidiani, in quelli più altamente tecnologici, fino a quelli più futuribili e inquietanti.

Durante i quattro giorni della manifestazione, stando ai dati forniti dagli organizzatori, è stato registrato un afflusso di circa 37.000 visitatori e, come l'anno precedente, un significativo numero di cittadini ed operatori, stimato in una media giornaliera di circa 550 utenti, ha visitato lo stand dell'Autorità dove erano in distribuzione le pubblicazioni curate dal Servizio relazioni con i mezzi di informazione. In particolare: la raccolta delle linee-guida del Garante, l'opuscolo "Dalla parte del paziente. *Privacy*: le domande più frequenti", la ventunesima edizione del Dvd "Il Garante e la protezione dei dati personali".

A Milano, il 29 marzo, si è tenuto il "*Cloud Forum* 2011". Il presidente Pizzetti ha richiamato l'attenzione sulle criticità e le questioni irrisolte legate alla "nuvola", in particolare sui rischi connessi all'archiviazione e al trattamento dei dati presso *server* situati in Paesi che potrebbero non assicurare le stesse rigorose tutele e garanzie a protezione dei dati previste nell'Unione europea.

Il tema del delicato rapporto tra protezione della vita privata e diritto di cronaca è stato altresì affrontato sia da Mauro Paissan al convegno "La memoria lunga della rete: *privacy*, reputazione e diritto all'oblio" svoltosi a Roma il 23 giugno 2011 e organizzato dal Cnr di Pisa e dell'Associazione nazionale stampa *online*, sia da Francesco Pizzetti, relatore all'incontro "Libertà di stampa e tutela della *privacy*" organizzato dall'Associazione stampa parlamentare il 28 novembre 2011 a Roma.

19.6. LE RELAZIONI CON IL PUBBLICO

Anche nel 2011, in linea con il principio di trasparenza amministrativa introdotto dalla l. 7 agosto 1990, n. 241, l'Autorità ha confermato il suo importante ruolo di tutela dei diritti della persona, anche garantendo elevati *standard* qualitativi nel servizio offerto quotidianamente.

L'azione dell'Urp, finalizzata all'efficienza ed al continuo dialogo, costituisce una quotidiana verifica dell'attività esplicata dall'Autorità in termini di risposta e soddisfazione dell'utenza, le cui numerose sollecitazioni trovano sbocco naturale nei provvedimenti emanati dall'Autorità stessa.

Le esigenze manifestate dal cittadino in ordine all'attività amministrativa vengono soddisfatte attraverso la collaborazione del personale dell'Ufficio, che favorisce il costante

aggiornamento in merito allo stato delle istruttorie in corso e fornisce delucidazioni sul complesso rapporto tra la normativa in materia di protezione dati personali ed il contesto normativo.

Altrettanto rilevante è stata la funzione informativa di tipo interno svolta dall'Ufficio, rivolta soprattutto alla individuazione delle macroaree di criticità e di interesse.

L'attività dell'Ufficio relazioni con il pubblico

La rapida trattazione delle richieste provenienti dai cittadini ha consentito all'Ufficio l'individuazione e la sintesi delle problematiche più rilevanti, per la sollecita e tempestiva elaborazione di soluzioni. La completezza delle informazioni così rese, la loro immediatezza e l'elasticità delle risposte sono state apprezzate dall'utenza come tratti distintivi e qualificanti del servizio prestato.

Le articolate funzioni dell'Ufficio sono riconducibili a tre grandi aree:

- orientamento: mediante la trasmissione di precedenti ricorrenti e modelli di istanza, l'Ufficio favorisce un approfondimento della tematica di interesse tramite la documentazione messa a disposizione e offre assistenza al cittadino nell'individuazione dello strumento di tutela più adatto al caso di specie;
- comunicazione e gestione integrata dei rapporti con l'utenza: la raccolta delle segnalazioni e delle sollecitazioni consente di vagliare le tematiche di maggiore interesse, poi oggetto dell'attività procedimentale nonché di interventi mirati dell'Autorità;
- informazione al cittadino: attraverso un rapporto diretto e dedicato presso la sede del Garante ovvero mediante il contatto telefonico e la posta elettronica. Risulta al riguardo essere gradita ed efficace l'attività di guida alla navigazione sul sito *web* dell'Autorità.

In virtù della continua ottimizzazione nello svolgimento dei compiti appena ricordati, anche nel trascorso anno l'Ufficio ha ricevuto frequenti manifestazioni di apprezzamento del servizio erogato, confermando il positivo riscontro dimostrato dai cittadini (rapporto "qualità erogata" e "qualità percepita").

Sulle diverse tipologie di quesiti ed istanze, ove necessario, anche attraverso ripetuti contatti con gli utenti, l'Urp svolge un'azione di capillare supporto, che inizia con la valutazione dei presupposti delle iniziative degli interessati e prosegue fino alla presentazione dell'istanza formale in stretto collegamento con l'unità organizzativa competente.

Di particolare rilievo è stata, in questo senso, l'attività di prima analisi delle migliaia di segnalazioni pervenute, relative al *telemarketing* (quelle arrivate tramite posta elettronica hanno fatto registrare nel 2011 un incremento del 18% rispetto al 2010), anche per richiedere agli interessati eventuali integrazioni prima dell'inoltro alle unità organizzative competenti. Il mutato quadro normativo, con l'istituzione del Registro pubblico delle opposizioni (v. Relazione 2010, p. 9 e ss.; p. 250 e ss.), ha infatti richiesto una cospicua attività informativa, non solo nel periodo transitorio e di prima applicazione, ma anche successivamente, a fronte di una vasta area di violazione delle nuove regole da parte di operatori economici, per l'individuazione dello strumento di tutela ritenuto più opportuno in ragione del singolo caso in esame.

Questa impegnativa attività preliminare ha favorito la conclusione nel corso dell'anno di numerose istruttorie, nonché l'adozione dei numerosi provvedimenti e relative richieste di sanzioni a carico dei trasgressori (v. al riguardo par. 9.1.)

L'apporto dell'Urp tuttavia non si esaurisce nella fase preliminare della presentazione dell'istanza, ma può comprendere ulteriori elementi di chiarimento e integrazione, dalla semplice richiesta di conoscere lo stato dell'istruttoria all'accesso agli atti ai sensi della l. n. 241/90.

L'analisi dei dati statistici relativi all'attività dell'Urp conferma che l'attenzione dell'utenza nei confronti di tematiche attinenti alla protezione dei dati è in costante aumento. Nell'ambito dell'attività di *front-office*, infatti, i contatti registrati nel periodo di riferimento sono pari a 31.921 (contatti telefonici, e-mail, visitatori, fascicoli), di cui oltre 31.200 avvenuti telefonicamente e per posta elettronica. A questi dati vanno aggiunti 235 fascicoli trattati nel corso del 2011.

In particolare, i contatti avvenuti attraverso il *call center* o direttamente ai numeri di telefono messi a disposizione dei cittadini (anche mediante diffusione sul sito *web* istituzionale) sono stati circa 13.000.

Nel corso dell'anno, 472 persone si sono recate presso l'Ufficio per ottenere informazioni su quesiti a carattere giuridico o per depositare atti. Anche in tali circostanze è stato distribuito materiale informativo e documentazione.

L'Ufficio ha ricevuto complessivamente 18.449 quesiti per e-mail e per posta ordinaria: la trattazione è avvenuta, nella gran parte dei casi, in 1 o 2 giorni lavorativi in tal modo garantendo, oltre all'accuratezza della risposta, un buon livello di immediatezza.

I dati elaborati dall'Ufficio consentono peraltro non solo di analizzare la tipologia delle richieste, ma anche di valutare l'eterogenea composizione dell'utenza e di calibrare le risposte in modo più adeguato alle caratteristiche dell'istante.

Anche per il 2011 si è riscontrato che, da parte di un certo numero di utenti, al primo contatto ne sono seguiti altri, mirati all'approfondimento della conoscenza di norme e provvedimenti dell'Autorità: ciò ha consentito un approccio dinamico ed esaustivo alle problematiche sottoposte all'Ufficio.

In questi specifici casi la tempistica e la qualità del servizio risultano di primaria importanza, ciò spiega la costante attenzione al miglioramento delle procedure interne, anche attraverso l'immediata comunicazione alle unità organizzative competenti ed ai vertici istituzionali –se del caso– per la gestione dell'emergenza.

Tematiche d'interesse

L'esame dei dati elaborati dall'Ufficio ha consentito di individuare le tematiche più ricorrenti, oggetto di attenzione da parte di cittadini e pubbliche amministrazioni.

Anche nel 2011, il più alto numero di richieste di chiarimenti e di segnalazioni ha riguardato il trattamento dei dati personali nell'ambito dell'attività di *marketing*. A seguito delle modifiche normative si è osservato un picco di contatti da parte sia degli operatori di settore, per chiarimenti sulla corretta predisposizione di procedure ed adempimenti, sia dei cittadini, non solo in relazione al *telemarketing*, ma anche agli altri strumenti utilizzati per le comunicazioni pubblicitarie non desiderate. L'esame delle segnalazioni relative alle telefonate commerciali e specificamente al *direct marketing*, ha innanzitutto evidenziato che, in diversi casi, il numero delle telefonate ricevute dagli utenti è aumentato e le modalità sono peggiorate (orari di ricezione, insistenza, scorrettezze contrattuali quali attivazione di un servizio non richiesto).

Dall'analisi delle segnalazioni e dei contatti telefonici si coglie, rispetto agli anni passati, una maggiore consapevolezza dei propri diritti, testimoniata dal contenuto delle richieste pervenute, più definito e circostanziato rispetto agli anni precedenti.

Anche le questioni relative all'applicazione del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 [doc. *web* n. 1712680], hanno continuato a rivestire grande interesse, in relazione sia al settore pubblico sia a quello privato. Numerose richieste hanno riguardato il controllo a distanza dei lavoratori, l'installazione di telecamere in ambito condominiale e in generale l'utilizzo della videosorveglianza per fini personali.

In virtù dei numerosi interventi e richiami dell'Autorità in merito al trattamento dei dati personali nell'ambito dell'attività giornalistica, risultano molto numerose le sollecitazioni dell'utenza finalizzate ad ottenere chiarimenti. Come già negli anni precedenti, la diffusione delle testate giornalistiche *online* ha comportato l'esigenza di fornire chiarimenti in merito al corretto esercizio del diritto di cronaca ed al diritto all'oblio in internet, oltre che riguardo agli strumenti di tutela adeguati ai singoli casi.

Il massivo ricorso ad innovative forme di comunicazione, quali i *social network* (*Facebook, MySpace*, ecc.) ha comportato un crescente interesse per la protezione dei dati personali, in particolare a tutela degli utenti di giovane età.

La grande eco che i mezzi di informazione attribuiscono ad alcune questioni di particolare impatto sulla sfera della riservatezza delle persone ha comportato un considerevole picco di richieste di chiarimenti ed approfondimento, ovvero talvolta, la manifestazione di valutazioni critiche.

Anche sulla scorta delle reazioni, spesso immediate, della pubblica opinione alle sollecitazioni provenienti dai *media,* il Garante è intervenuto frequentemente in merito al trattamento dei dati personali nell'ambito dell'attività di informazione e giornalistica, anche in relazione a pratiche contrarie alla deontologia professionale e lesive della sfera di riservatezza non solo di personaggi pubblici, ma soprattutto di soggetti socialmente deboli ed esposti, quali i minori, i malati, le persone vittime di reati o coinvolte, a vario titolo, in indagini giudiziarie.

Con riferimento al trattamento dei dati nella gestione del rapporto di lavoro, si segnalano sia specifiche richieste di intervento e di tutela del lavoratore, sia semplici richieste di informazioni e chiarimenti sulla normativa applicabile.

Per quanto riguarda il settore pubblico, le tematiche più ricorrenti sono state quelle della trasparenza e dell'accesso ai documenti amministrativi, della diffusione dei dati personali del

lavoratore, del trattamento dei dati sanitari dello stesso, ma anche dei suoi familiari, nonché dei rapporti con le organizzazioni sindacali.

Comuni al settore pubblico e privato sono le problematiche legate al trattamento dei dati biometrici dei lavoratori (anche per la semplice rilevazione delle presenze), all'uso degli strumenti elettronici sul luogo di lavoro (posta elettronica e internet), alla geolocalizzazione, oltre che alla già citata videosorveglianza.

Permane di interesse il trattamento dei dati personali in ambito bancario e, più in generale, del credito e degli investimenti, anche con chiarimenti e interventi relativi a problematiche sorte negli ultimi anni in relazione all'entrata in vigore di norme riguardanti la valutazione dell'adeguatezza e dell'appropriatezza delle operazioni o dei diversi servizi di investimento forniti (Direttive n. 2004/39/CE e n. 2006/73/CE), nonché in relazione all'adozione della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231).

Ancor più frequenti sono state le richieste di assistenza per attivare le procedure di intervento a correzione delle informazioni personali trattate da parte dei sistemi informativi privati in materia di credito al consumo e puntualità e affidabilità nei pagamenti.

Un considerevole numero di richieste di chiarimenti è pervenuto anche in ordine alle modalità di trattamento dei dati personali connesse al 15° Censimento generale della popolazione e delle abitazioni.

19.7. IL SERVIZIO STUDI E DOCUMENTAZIONE

La redazione della Relazione annuale

Il Servizio studi ha coordinato la redazione del testo della Relazione annuale, la cui presentazione al Parlamento, costituisce un fondamentale adempimento istituzionale dell'Autorità. La preparazione del resoconto sull'attività svolta nel corso dell'anno è un'importante occasione di riflessione all'interno dell'Ufficio, anche ai fini di possibili miglioramenti dello svolgimento delle funzioni del Garante, ivi compresa la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali.

La funzione di studio e di supporto giuridico

Il Servizio studi ha continuato a svolgere attività di studio e ricerca su questioni tecnico-giuridiche di interesse dell'Autorità anche su impulso del Collegio, del segretario generale nonché delle strutture dell'Ufficio.

Le questioni esaminate riguardano, tra l'altro, la legittimazione di testate giornalistiche ad accedere a documenti amministrativi ai sensi della l. n. 241/1990, la rilevanza della disposizione costituzionale inerente al dovere dei cittadini di adempiere con disciplina ed onore le funzioni pubbliche loro affidate (art. 54, comma 2, Cost.), la possibilità per l'interessato di delegare l'accesso al fascicolo sanitario elettronico, con l'eventuale individuazione delle relative modalità, la pubblicabilità integrale di messaggi di posta elettronica scambiati tra gli utenti di una *mailing list* di magistrati, l'applicabilità della *prorogatio* al Collegio del Garante, la revisione della Convenzione n. 108/1981 del Consiglio d'Europa (sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale), nonché la disciplina delle foto scattate dalle tribune stampa di testi scritti da parlamentari non destinati ad usi istituzionali.

Il Servizio studi ha inoltre coadiuvato l'attività istituzionale del Garante attraverso la ricerca e la trasmissione alle strutture interessate, di documentazione nazionale ed internazionale nonché di sintetiche osservazioni su questioni d'interesse, quali le incursioni abusive nella vita privata altrui attraverso strumenti tecnologici molto sofisticati, sanzionate ai sensi dell'art. 615-*bis* c.p..

I pareri sulle leggi regionali

Il Servizio ha altresì costantemente fornito, a mezzo di atti interni, elementi di valutazione per i pareri richiesti dalla Presidenza del Consiglio dei ministri, ai fini dell'eventuale impugnazione di leggi regionali davanti alla Corte costituzionale, ai sensi dell'art. 127 Cost.. Le menzionate valutazioni riguardano, previ approfondimenti normativi, giurisprudenziali ed eventualmente dottrinali, la conformità delle leggi regionali alla disciplina sulla protezione dei dati personali.

Come negli anni precedenti, i testi legislativi esaminati sono risultati, di massima, rispettosi dei limiti di cui all'art. 117 Cost., anche alla luce di quanto deciso dalla Consulta (sent. n. 271/2005) sulla competenza legislativa esclusiva dello Stato in materia di *privacy*, nonché dei princìpi e delle disposizioni contenuti nella normativa internazionale (art. 8 CEDU) e comunitaria.

Più in dettaglio, oltre alla segnalazione alla Presidenza del Consiglio dei ministri dei profili di dubbia costituzionalità relativi ad una legge regionale, di cui si è già riferito (v. par. 1.3.),

tra i testi più problematici si cita una legge regionale in materia di istruzione e formazione professionale, soprattutto in ragione di una disposizione che parrebbe consentire alla giunta la raccolta di dati, anche sensibili, relativi a singoli studenti in assenza di una norma statale.

Oggetto di approfondimento è stata altresì una legge regionale che ha, in particolare, esteso ai dirigenti della Giunta e del Consiglio (ovvero a personale amministrativo, seppure apicale) il regime di pubblicità della situazione patrimoniale e tributaria previsto per i consiglieri e gli assessori. Ciò per diversi profili: da un lato, per la possibile diffusione di dati personali, anche di natura sensibile, quali informazioni sulla salute o sull'appartenenza a sindacati o partiti, spesso oggetto di dichiarazioni inerenti al reddito; dall'altro, perché la legge è apparsa difforme dalla normativa nazionale che legittima le regioni a legiferare nella materia in parola unicamente rispetto a persone che rivestono cariche elettive (cfr. art. 15, l. n. 441/1982). Nel caso di specie, l'interesse pubblico alla divulgazione della situazione patrimoniale dei dirigenti non è stato apparso prevalente sul diritto degli stessi alla riservatezza, trattandosi di dati di persone estranee ad un rapporto di rappresentanza politica (v. anche par. 1.3.).

Un cenno in questa sede merita infine una legge in materia di tracciabilità informatica del procedimento amministrativo, soprattutto in riferimento ad alcune disposizioni volte ad assicurare la trasparenza amministrativa. In particolare, le perplessità hanno riguardato la possibile estensibilità, in via di interpretazione, dell'accesso agli atti infraprocedimentali, in violazione del principio di essenzialità, nonché la genericità della previsione sulla tracciabilità dell'utilizzo delle sovvenzioni regionali, che non è apparsa in armonia con l'esigenza di bilanciare l'interesse a garantire la trasparenza dell'amministrazione pubblica con i diritti al rispetto della vita privata e alla protezione dei dati personali.

I servizi interni di documentazione

Il Servizio studi, in conformità alle proprie competente regolamentari, ha curato l'aggiornamento del personale attraverso la redazione di due notiziari interni:

il "Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona" denominato "Osservatorio *privacy*", una rassegna periodica di normativa, dottrina e giurisprudenza nazionale comunitaria ed internazionale su questioni di interesse per l'Autorità, suddivisa in un'ampia sezione di princìpi generali e in quattro sezioni più

specialistiche, corrispondente alle macroaree tematiche di attività del Garante: libertà pubbliche e sanità; comunicazione e reti telematiche; realtà economiche e produttive; amministrazione, contratti e risorse umane;

il "Servizio studi news", strumento di monitoraggio delle novità nella giurisprudenza, anche comunitaria ed internazionale in materia di diritti e libertà delle persone e protezione dei dati personali, in un contesto nel quale giudici ed autorità di sistemi giuridici diversi valutano i casi alla luce di concorrenti princìpi di carattere generale (cfr. artt. 8 e 10 CEDU, come applicati per es. da CEDU 25 gennaio 2011, in Reinboth and Others v. Finland, in http://www.echr.coe.int/ECHR/Homepage_EN).

19.8. LA BIBLIOTECA

La Biblioteca nasce nel 2001 e rappresenta un'articolazione della Segreteria generale. Il suo compito istituzionale consiste nella raccolta e nella conservazione delle pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati. In raccordo con il dettato normativo, l'incremento del patrimonio della biblioteca si estende alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale. Un campo di particolare rilievo è costituito dalla storia della vita privata nell'età moderna e dalle matrici extragiuridiche, religiose e letterarie, del *right to privacy*. In collaborazione con il Dipartimento risorse tecnologiche viene poi istituito un fondo speciale di testi scientifici sulle tecnologie dell'informazione in rapporto alla protezione dei dati.

Attualmente la Biblioteca possiede ca. 11.000 volumi (circa 6.000 in lingua straniera), 400 testate di periodici cartacei (35 correnti) e 200 tesi di laurea e di dottorato.

Nel corso del 2011 è proseguito l'ampliamento del patrimonio con l'acquisto o il ricevimento gratuito delle principali pubblicazioni monografiche in materia di protezione dei dati, con priorità assegnata alla produzione italiana e subordinatamente alla produzione tedesca e statunitense. Particolare attenzione è stata attribuita alla tematica delle intercettazioni telefoniche oggetto di una specifica sezione della Biblioteca. È stata intensificata la raccolta delle pubblicazioni a stampa delle autorità di protezione dei dati in Europa e nel mondo. È continuato lo spoglio sistematico dei titoli analitici in materia di protezione dei

dati che appaiono in monografie e periodici italiani e stranieri: questo settore di acquisizione si avvale di *database online* che facilitano, in particolare, il monitoraggio dei periodici giuridici di lingua inglese.

Come anticipato nella Relazione dello scorso anno, l'esigenza di riordinare sulla base di nuovi criteri il vasto patrimonio bibliografico raccolto nell'arco di oltre un decennio ha condotto alla stesura di due documenti specifici, la Carta delle collezioni e il Regolamento. La prima descrive gli indirizzi per l'incremento del posseduto, evidenziando in dettaglio i settori disciplinari presenti in catalogo e indicando le aree di possibile espansione. Il secondo delinea gli scopi e le modalità di funzionamento della Biblioteca, principalmente per quanto concerne l'utenza interna.

Il progetto di *Digital Library*, avviato nel 2008 in cooperazione con il Dipartimento risorse tecnologiche, costituisce il principale fattore qualificante del programma di riorganizzazione varato nel 2009 e in corso di attuazione. Accanto alle "strategie di possesso" (imperniate sull'incremento del patrimonio cartaceo) sono state perfezionate nuove "strategie di accesso" concentrate per l'acquisizione di archivi *full-text* pubblicati in formato elettronico. Il sito *web* della Biblioteca, trasformato in portale, è stato suddiviso in aree funzionali in modo da coordinare tutte le risorse bibliografiche elettroniche (l'OPAC *online* e i *database*) nel quadro di una *knowledge infrastructure*: questa architettura di conoscenze condivise è al servizio delle attività di studio e di ricerca intraprese dalla presidenza e dai componenti del Collegio e, in parallelo, fornisce una serie di strumenti informativi qualificati per le attività dei dipartimenti e dei servizi nei rispettivi settori di competenza.

Il forte ampliamento dei moduli dei *database* e l'inserimento della formula della multiutenza sulla rete intranet, come rappresentato anche nella precedente Relazione, ha permesso di ottimizzare la condivisione delle risorse, aumentando il numero delle banche dati giuridiche di accesso *web* e di accesso remoto rese disponibili su tutte le postazioni dell'Ufficio.

Nel 2011 le richieste di titoli in lettura da parte di utenti interni sono state 4.430: le domande di frequentazione di utenti esterni assommano a 138, con circa 1.720 richieste di titoli in lettura. I contatti sul catalogo OPAC sono stati 5.800 e 244 i casi di assistenza bibliografica e di *documents delivery* effettuati *online*.

In questo quadro i dati analitici relativi alla consultazione dei *database* da parte della utenza interna consolidano il trend di crescita registrato nel biennio 2009-2010 e assumono valenza anche di indicatori qualificati di una nuova fase della produttività dell'Ufficio. Per quanto riguarda le tre banche dati giuridiche di maggiore rilevanza il numero globale delle sessioni è stato di 9.387 (con una media giornaliera lavorativa di 42 connessioni). Il *database* che registra il più elevato conteggio statistico totalizza 4.889 sessioni di lavoro (4.052 nel 2010) e 60.141 documenti consultati (48.112 nel 2010), pari a una media giornaliera lavorativa di 22 connessioni e 273 documenti.

L'Ufficio del Garante

III. L'Ufficio del Garante

20. LA GESTIONE AMMINISTRATIVA DELL'UFFICIO

20.1. IL BILANCIO E LA GESTIONE FINANZIARIA

Le risorse finanziarie acquisite al bilancio del Garante sono state utilizzate per lo svolgimento dei compiti istituzionali dell'Ufficio e per il perseguimento degli obiettivi programmatici definiti in sede di approvazione del bilancio di previsione per il 2011, nel rispetto delle procedure di legge e regolamentari che disciplinano la materia.

La gestione amministrativa ha fatto registrare un significativo incremento delle entrate complessive di competenza, rispetto a quelle acquisite nel precedente esercizio, nella misura di circa 7,2 milioni di euro.

Infatti, le entrate totali affluite al bilancio del Garante sono state complessivamente 23,8 milioni di euro a fronte dei 16,6 milioni di euro del precedente esercizio.

Tale incremento è dovuto al contributo, pari a 12,0 milioni di euro, erogato da altre Autorità amministrative indipendenti in esecuzione di una specifica disposizione, contenuta nell'art. 1, comma 241, della legge 23 dicembre 2009, n. 191. L'entità del menzionato contributo, previsto soltanto per gli anni 2011 e 2012, ha consentito di assicurare il necessario equilibrio finanziario dell'Autorità per gli anni in questione.

Tale entrata costituisce anche il provento più significativo, rappresentando oltre il 50% del totale delle risorse finanziarie acquisite al bilancio dell'Autorità.

Lo stanziamento erogato a valere sul bilancio dello Stato, invece, ammonta a 8,5 milioni di euro, la cui misura, in forte riduzione rispetto a quella dei precedenti esercizi, rappresenta ora soltanto il 35,88% del totale delle entrate, a conferma di un costante ridimensionamento delle risorse poste a carico della finanza pubblica per assicurare il funzionamento dell'Ufficio.

Ulteriori fonti di finanziamento sono assicurate dai proventi affluiti al bilancio del Garante, derivanti dalle sanzioni pecuniarie, il cui importo per il 2011 è pari a 1,5 milioni di euro, a fronte di 2,0 milioni di euro del 2010.

L'attività gestionale dell'Autorità si è svolta nel rispetto dei vincoli di spesa e degli indirizzi di contenimento previsti dalle disposizioni legislative intervenute in materia.

La spesa complessiva imputabile alla competenza dell'esercizio ammonta a 19,2 milioni di euro, con una significativa contrazione rispetto alle somme stanziate in sede di previsione.

Lo scostamento rispetto alle stime iniziali è di circa 3,9 milioni di euro e le economie gestionali sono state realizzate prevalentemente a carico di capitoli della spesa corrente mentre in misura meno rilevante su quelli accesi alle spese in conto capitale.

La gestione amministrativa dell'esercizio è stata caratterizzata anche dalla necessità di realizzare economie di spesa su singoli capitoli per i quali il legislatore ha previsto una specifica riduzione.

L'Ufficio, infatti, oltre ad osservare i limiti imposti alla spesa corrente su talune voci, tra le quali si segnalano quelle connesse, ad esempio, alla gestione delle autovetture ovvero per consulenze, nel 2011, ha applicato la prevista riduzione dei compensi degli organi, nella misura del 10%, e quella sugli emolumenti spettanti al personale per la parte eccedente gli importi complessivi annui di euro 90.000 e di euro 150.000 nella misura, rispettivamente, del 5 e del 10%. Peraltro, tali economie, ove previsto, sono state regolarmente versate a favore del bilancio dello Stato nel rispetto di puntuali disposizioni legislative.

La parte più significativa della spesa imputabile all'esercizio resta comunque ascrivibile a quella avente carattere fisso e continuativo, per la quale non appaiono praticabili interventi ulteriori rispetto a quelli comunque adottati dall'Ufficio.

La rimanente parte della spesa, connessa essenzialmente al funzionamento dell'Autorità, assume carattere più contenuto e la sua entità complessiva è stata comunque ricondotta entro i limiti previsti dalle disposizioni finanziarie di contenimento della spesa pubblica.

La spesa in conto capitale per l'acquisizione di beni aventi un'utilità pluriennale è stata anch'essa ridotta rispetto alle previsioni, la cui stima iniziale teneva conto dell'esigenza, poi non realizzatasi, di trasferire in corso d'anno la sede dell'Autorità.

Il perseguimento delle finalità istituzionali è avvenuto nel rispetto degli indirizzi di contenimento della spesa previsti dai richiamati provvedimenti legislativi e l'attività amministrativa dell'Autorità non ha subito rallentamenti.

La tabella allegata alla presente Relazione (par. 20., tab. 21) riassume sinteticamente i valori finanziari di competenza che hanno interessato la gestione nel 2011, posti a raffronto con quelli dell'esercizio precedente.

In particolare, la tabella espone le fonti di finanziamento complessive dell'anno, con evidenziazione degli importi posti a carico del bilancio dello Stato. Per quanto riguarda la spesa, l'onere complessivo sostenuto dall'Ufficio per lo svolgimento delle attività istituzionali trova separata evidenza tra la spesa connessa al funzionamento, comprensiva degli oneri per gli organi e per il personale, e quella per investimento e per rimborsi, nonché per restituzioni in favore del bilancio dello Stato. Accanto ai valori registrati nell'anno sono indicati, quelli del precedente esercizio, con evidenziazione in apposita colonna degli scostamenti registrati tra i due periodi.

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 ed in tale ottica si è proceduto, tra l'altro, a razionalizzare gli spazi, anche per esigenze di economicità della spesa.

20.2. L'ATTIVITÀ CONTRATTUALE E LA GESTIONE ECONOMALE

Per quanto attiene all'attività contrattuale, nel corso dell'anno 2011, mediante direttiva del segretario generale sono state ridefinite e razionalizzate le procedure interne e i flussi documentali relativi agli acquisti di beni e servizi, contemperando le esigenze di speditezza e snellezza procedurale con la precisa attribuzione delle funzioni di pertinenza delle singole unità organizzative dell'Autorità.

L'attività di selezione dei fornitori è stata esperita, nel rigoroso rispetto della vigente disciplina in materia di contratti pubblici, privilegiando, ove possibile, il ricorso a procedure comparative, anche di rilievo comunitario.

In particolare, si segnalano la gara per i servizi assicurativi dell'Autorità e la connessa procedura per la selezione del *broker*, nonché le procedure in materia di amministrazione digitale e quelle finalizzate ad assicurare l'ordinario funzionamento dell'Ufficio (tra le quali quelle relative all'affidamento dei servizi di pulizie e *reception* e di assistenza alle attività di protocollazione e catalogazione).

Per le diverse esigenze di carattere informativo-divulgativo sono stati predisposti gli atti di gara per l'individuazione di un unico fornitore dei servizi di stampa.

Di rilievo l'ulteriore implementazione delle procedure di acquisizione di beni e servizi mediante centrali di acquisto (Consip S.p.A., Digit PA), per le acquisizioni di buoni pasto, dei servizi di telefonia fissa, dei servizi di connettività, nonché attraverso il mercato elettronico della pubblica amministrazione (MEPA).

L'economicità e l'efficienza delle procedure comparative effettuate mediante tale ultimo strumento hanno consentito, anzitutto, di aumentare il numero ed il volume di acquisizioni tramite "Richiesta di offerta" (RDO), gestite in forma interamente telematica; tale procedura, inoltre, ha potuto trovare utile impiego anche in relazione ad acquisti di limitato importo, consentendo una maggiore apertura al mercato per beni solitamente oggetto di affidamenti "diretti" mediante procedura negoziata. Inoltre, anche gli ordini di affidamento diretto, sempre rigorosamente contenuti entro i limiti previsti dalla normativa, sono stati generalmente preceduti da ricerche di mercato effettuate mediante comparazione dei dati presenti sul MEPA, talché anche in tale fattispecie il confronto concorrenziale tra gli operatori economici è stato garantito, con i conseguenti vantaggi per l'Autorità nonché per il sistema complessivamente inteso.

In prossimità della scadenza del contratto di locazione dell'immobile destinato a sede del Garante, è stata effettuata una articolata attività di ricerca di mercato, al termine della quale è stato deciso il rinnovo del contratto in essere per ulteriori sei anni. Tale rinnovo ha visto l'acquisizione di nuovi spazi e, contestualmente, la cessione di altri all'interno dello stesso stabile al fine di ottimizzare la dislocazione degli uffici dell'Autorità.

In relazione alle cd. attività di economato, ossia, prevalentemente, di gestione della sede dell'Autorità, è stata effettuata una riorganizzazione funzionale, finalizzata ad una razionalizzazione delle competenze e ad una migliore definizione delle responsabilità tra gli uffici dell'Autorità che, a parità di risorse impiegate, consentirà un utilizzo più efficiente delle stesse.

Merita inoltre di essere menzionata la stipula di una convenzione di durata triennale con il Ministero degli affari esteri, nell'ambito del progetto di sviluppo e di sostenibilità del processo di dematerializzazione denominato "Progetto @doc" che, coerentemente con il Piano per

l'*e-government* 2012 che prevede l'attuazione del Codice dell'amministrazione digitale quale strumento di sviluppo dei servizi pubblici, tende a favorire il riuso di piattaforme tecnologiche esistenti presso le pubbliche amministrazioni.

Da segnalare, poi, che nel 2011 sono intervenute diverse modifiche normative nella materia degli appalti pubblici, di rango sia primario sia regolamentare, che hanno richiesto una costante attività di aggiornamento dell'Ufficio.

20.3. LE NOVITÀ LEGISLATIVE E REGOLAMENTARI E L'ORGANIZZAZIONE DELL'UFFICIO

Dato saliente del 2011 è stata l'attuazione delle misure di contenimento della spesa pubblica, in applicazione del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122.

In tale quadro, in attuazione del principio di invarianza del trattamento economico del personale, nel triennio 2011-2013, rispetto al 2010, le retribuzioni non hanno subìto incrementi e sono state operate le riduzioni dei trattamenti economici complessivi eccedenti, rispettivamente, 90.000 e 150.000 euro, nelle misure stabilite dal citato d.l. n. 78/2010 (art. 9, comma 2).

Sono state inoltre effettuate le previste riduzioni dei compensi corrisposti ai componenti del collegio e al segretario generale, nonché a tutti i titolari di incarichi presso l'Ufficio del Garante e sono state operate le riduzioni di spesa previste in materia di missioni all'estero, consulenze, partecipazione a convegni, sponsorizzazioni, spese di rappresentanza, formazione del personale, autovetture.

In particolare, per effetto di importanti decisioni organizzative volte a contenere ulteriormente le spese in materia, allo stato, l'Autorità non si avvale di consulenti e dispone della sola auto di servizio assegnata dal Ministero delle infrastrutture e trasporti per le esigenze di mobilità del presidente.

Nel 2011 sono stati rinnovati gli incarichi dirigenziali, confermando i tre vice-segretari generali individuati nel marzo 2010 al fine di assicurare il migliore svolgimento delle funzioni di coordinamento dell'Ufficio proprie del segretario generale. È stata inoltre istituita un'unità competente per le questioni riguardanti il trattamento di dati personali nell'ambito del rapporto di lavoro pubblico e privato.

Pur nel contesto di una sensibile riduzione dello stanziamento a disposizione dell'Autorità in relazione allo stato della finanza pubblica, nel 2011 sono stati immessi in servizio i vincitori della procedura selettiva per quattro funzionari con profilo giuridico da assumere con contratto a tempo determinato (G.U. –quarta serie speciale– 26 febbraio 2010, n. 16) e, in considerazione delle esigenze di servizio, è stata assunta la determinazione di effettuare lo scorrimento della graduatoria di merito per un'ulteriore unità.

Sono state, altresì, indette due procedure selettive per reclutare, rispettivamente, un funzionario a contratto (con possibilità di aggiungerne un altro) per l'area comunicazione, e due funzionari con profilo informatico, con contratto a tempo determinato. Tali procedure non hanno avuto seguito per i motivi, sopra esposti, attinenti alle contingenti difficoltà finanziarie.

Al fine di acquisire stabilmente nell'organico dell'Autorità personale già in servizio, in possesso di specifiche professionalità e di requisiti adeguati e comprovati nel tempo, nel dicembre 2011 è stata indetta una procedura di mobilità volontaria ai sensi dell'art. 30 del d.lgs. n. 165/2001, riservata al personale in posizione di fuori ruolo presso l'Ufficio da almeno un anno, per tre posizioni di funzionario e due di impiegato operativo.

L'attività di segreteria del Collegio

Nel 2011 il servizio di segreteria del Collegio ha curato tutti gli adempimenti necessari allo svolgimento delle attività di tale organo, provvedendo inoltre alla conservazione dei verbali delle riunioni, degli originali delle deliberazioni adottate e del materiale utile per le pubblicazioni sulla Gazzetta Ufficiale. Particolare cura ha richiesto, in stretto raccordo con le diverse unità organizzative dell'Ufficio, la definizione dei testi deliberati, destinati –tramite la redazione *web*– alla pubblicazione sul sito istituzionale dell'Autorità.

Nel corso dell'anno è stato messo a punto il registro interno delle deliberazioni collegiali, classificate in ragione della materia, ferma restando la prevista fascicolazione di archivio. La procedura di registrazione si avvale di un apposito programma informatico, creato appositamente per *database* relazionali.

In questo modo è accresciuta l'efficacia del lavoro in team, in particolare per quanto riguarda la ricerca di atti articolata per numero di riunione, per anno, per tipologia di provvedimento o ancora combinando i detti criteri, assicurando nel contempo la necessaria sicurezza, tramite la delimitazione degli accessi e le procedure di autenticazione.

20.4. IL PERSONALE E I COLLABORATORI ESTERNI

Nel 2011 sono state immesse in servizio complessivamente cinque unità a contratto in qualità di vincitori della sopra descritta procedura selettiva per quattro funzionari con profilo giuridico da assumere con contratto a tempo determinato. Tale procedura, ultimata nel 2010, era volta alla copertura dei posti ancora vacanti nel contingente di 20 posti di personale con contratto a tempo determinato, previsto dall'art. 156, comma 5, del Codice.

Nel dicembre del 2011 è stata avviata la procedura di mobilità volontaria, riservata al personale in posizione di fuori ruolo in servizio presso l'Ufficio, a complessivi cinque posti, di cui tre per posizioni di funzionario e due per posizioni di impiegato operativo.

Nel periodo considerato si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2011, l'Ufficio poteva contare su un organico, a diverso titolo, di 109 unità, di cui 103 in servizio, al quale va aggiunto un contingente di personale a contratto di 20 unità, alcune delle quali peraltro assunte per brevi periodi.

Dai suddetti dati si evidenzia che nell'anno considerato si è verificato un contenuto incremento del personale in servizio rispetto all'anno precedente.

Nel periodo in esame, l'Autorità si è avvalsa delle figure professionali previste dalla vigente normativa in materia di sicurezza e incolumità dei lavoratori nei luoghi di lavoro (medico competente e responsabile del servizi di prevenzione e sicurezza).

Presso l'Autorità opera il servizio di controllo interno che è 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.

20.5. IL SETTORE INFORMATICO E TECNOLOGICO

Sviluppo del sistema informativo e dei servizi ICT

Nel 2011 è proseguita l'attività di consolidamento del sistema informativo avviata negli scorsi anni, su linee di sviluppo all'insegna dell'*open source* (già ampiamente utilizzato), del riuso e dei formati aperti.

È continuata l'opera di ammodernamento e razionalizzazione dell'infrastruttura informatica, per la riduzione dei costi di gestione dei sistemi informatici, potenziando ulteriormente la piattaforma di virtualizzazione *VMware* tramite cui sono erogati quasi tutti i servizi basati

su *server Windows* o *Linux*, oltre ai sistemi di *storage* accessibili con tecnologia *Fibre Channel* nell'ambito di una *Storage Area Network*. La centralizzazione ed il successivo aggiornamento delle procedure di *backup/restore* dei dati hanno consentito una migliore efficienza nella loro gestione.

È proseguita altresì la digitalizzazione della Biblioteca, con l'erogazione di servizi sulla rete intranet per la consultazione di *database* bibliografici e di riviste *online*, oltre alla pubblicazione dell'OPAC (tramite il *software Sebina Open Library*) e di una rinnovata area dedicata nella intranet.

È stato ulteriormente sviluppato l'uso interno della piattaforma intranet per l'Ufficio, basata sull'infrastruttura *Microsoft Sharepoint*, oltre che l'utilizzo della firma digitale tramite la carta nazionale dei servizi e della posta elettronica certificata (PEC).

È stato avviato un accordo di collaborazione con il Ministero degli affari esteri per il riuso della piattaforma "documentale @doc", basata sul sistema di gestione dei *workflow* documentali "Alfresco", che consentirà, una volta configurata e personalizzata, di smaterializzare i principali flussi documentali relativi ai procedimenti amministrativi.

È stato avviato un progetto di rinnovamento del sito *web* dell'Autorità.

Per l'ammodernamento della rete interna sono stati acquistati nuovi apparati di rete ed è stata potenziata l'ampiezza di banda, accrescendo l'efficienza nelle attività lavorative.

Impegno per la sicurezza informatica dell'Ufficio

Anche nel 2011 nessun incidente informatico di rilievo è occorso nel dominio dell'Ufficio, e in particolare nessun evento relativo alla sicurezza ha prodotto danni o disservizi. Nessun virus informatico è penetrato nella rete interna attraverso canali di rete mentre i controlli sui trasferimenti da supporti hanno consentito di bloccare ogni contenuto nocivo rilevato. Non si sono verificate perdite di dati sottoposti a *backup*, e alle occasionali indisponibilità o cancellazione accidentali di file o di documenti è stato possibile quasi sempre porre rimedio con le ordinarie procedure o con i servizi di assistenza.

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento risorse tecnologiche ha fornito nel 2011 supporto consultivo all'Ufficio, formulando analisi tecniche per le fasi istruttorie dei procedimenti e per la redazione dei provvedimenti dell'Autorità, e ha curato con note informative e relazioni l'approfondimento di argomenti a contenuto informatico-tecnologico. Ha inoltre partecipato a incontri e

riunioni di lavoro, preliminari a interventi dell'Autorità in convegni o su organi di stampa, nel corso dei quali sono stati affrontati i profili tecnologici di temi di pubblico interesse. In particolare si evidenziano, nell'ambito delle telecomunicazioni e di internet: la collaborazione per la stesura della scheda informativa "Smartphone e tablet: scenari attuali e prospettive operative" allegata alla Relazione 2010; la consulenza in merito a tecnologie e servizi emergenti legati alla geolocalizzazione; la consulenza nell'elaborazione del provvedimento del Garante relativo alle cd. "telefonate mute" nel *marketing* dei servizi elettrici; la collaborazione al parere reso all'Autorità per le garanzie nelle comunicazioni sulla costituzione di una *black list* dei clienti telefonici morosi; l'attività volta a ridurre l'incidenza della ricezione di fax di disturbo, provenienti da *provider* stabiliti al di fuori del territorio nazionale, l'attività inerente alle misure di sicurezza nell'ambito dell'attivazione di servizi di televisivi a pagamento su piattaforme digitale terrestre; le attività volte a limitare l'uso di dati identificativi degli utenti nell'ambito della profilazione, da parte degli operatori telefonici.

Nell'ambito della collaborazione relativa a provvedimenti riguardanti il settore pubblico e il rilascio di pareri a ministeri e organismi governativi, si evidenziano, oltre a quanto già riportato nella Relazione 2010, i principali atti che hanno richiesto l'elaborazione di analisi e rapporti tecnici: parere tecnico sul nuovo regolamento del Ministero dell'interno relativo all'Indice nazionale delle anagrafi (INA); parere tecnico e relativa attività istruttoria su carta multiservizi difesa; parere tecnico sullo schema di d.P.C.m. recante regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (ai sensi degli artt. 20, comma 3; 24, comma 4; 28, comma 3; 32, comma 3, lettera *b*); 35, comma 2; 36, comma 2 e 71, del codice dell'amministrazione digitale - CAD); parere tecnico sullo schema di provvedimento recante regole tecniche per la consultazione ed estrazione di indirizzi PEC ed elenchi di indirizzi PEC di cui all'art. 6, comma 1-*bis*, del CAD; parere tecnico sullo schema di provvedimento del responsabile per i sistemi informativi automatizzati del Ministero della giustizia concernente specifiche tecniche del decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, recante il regolamento sulle regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione; convenzione del Ministero dell'interno con l'Agenzia delle entrate per il

collegamento del Sistema informativo *interforze* al sistema "Puntofisco"; parere sulla convenzione tra Direzione investigativa antimafia e INAIL.

Per quanto riguarda le attività orientate alle realtà economiche e produttive, il Dipartimento ha fornito supporto nell'elaborazione dei provvedimenti adottati dal Garante in tema di circolarità e tracciabilità delle operazioni nelle banche e in tema di trattamento dei dati relativi alla navigazione in internet dei dipendenti di una società.

Contributi all'attività ispettiva

È stato fornito continuativo e proficuo supporto ad importanti attività ispettive, con la realizzazione di accessi a banche dati, con l'analisi e lo studio dei materiali acquisiti, con la stesura di rapporti e con la formulazione di misure e accorgimenti di natura tecnologica. Tra le attività più significative in questo ambito si segnalano la campagna esplorativa sui servizi *cloud* nazionali; le ispezioni su catene alberghiere per la verifica dei trattamenti dei dati personali nell'ambito dei circuiti di pagamento con carta di credito; le ispezioni propedeutiche all'adozione del provvedimento sulle cd. "chiamate mute" nel *telemarketing*. (vedi par. 17.3).

Contributi all'attività internazionale

Il Dipartimento ha partecipato all'attività internazionale dell'Autorità nell'ambito sia dei gruppi di esperti nominati dalla Commissione europea su temi specifici, sia delle attività istituzionali del Gruppo Art. 29, con studio di documenti e produzione di rapporti. Si segnalano in particolare, nell'ambito delle attività di tale Gruppo, la partecipazione ai lavori del *Technology Subgroup*, che affronta le tematiche di attualità nell'area ICT in materia di protezione dei dati personali. Di rilievo, in tale ambito, sia il contributo fornito all'attività del Gruppo Art. 29 relativa al recepimento, da parte degli Stati membri, della Direttiva n. 24/2006/CE sulla *data retention*, sia la produzione di rapporti e relazioni tecniche connesse alla revisione del quadro normativo e*Privacy*, come modificato dalla Direttiva n. 136/2009/CE.

Il Dipartimento ha poi rappresentato l'Autorità nel Gruppo di Berlino per le telecomunicazioni, partecipando alle due riunioni svoltesi nel 2011 e contribuendo alla redazione di documenti ufficiali del Gruppo, in particolare, sul tema del diritto all'oblio, fornendo una approfondita analisi sull'applicazione di appositi protocolli informatici da parte dei gestori dei siti *web*. L'approvazione definitiva del documento è attesa entro il 2012 (vedi par. 18.4.).

Attività informativa e di divulgazione

Il Dipartimento ha presentato relazioni a seminari, *workshop* e convegni sugli aspetti tecnologici della protezione dei dati personali. Tra gli interventi più significativi si menzionano

quelli nell'ambito del *Forum Pa* 2011 e al convegno ICT *Security 2011*. Una menzione particolare merita il contributo recato al corso di formazione tecnica rivolto al Nucleo *Privacy* della Guardia di finanza.

Il Dipartimento ha inoltre offerto continuo supporto, in collaborazione con l'Urp, nelle risposte a quesiti e richieste di chiarimento relative a normativa e provvedimenti del Garante in tema di sistemi ICT, e ha contribuito in modo significativo alla redazione della scheda informativa "*Cloud computing*: indicazioni per l'utilizzo consapevole dei servizi" allegata alla Relazione 2010.

20.6. IL MONITORAGGIO DELL'EFFICACIA E DELL'EFFICIENZA E IL SUPPORTO AL CONTROLLO INTERNO

Anche per l'anno 2011, l'Unità raccolta dati, flussi informativi e supporto al controllo interno ha effettuato il monitoraggio delle attività svolte dalle unità organizzative dell'area giuridica e dall'Ufficio relazioni con il pubblico, raccogliendo informazioni e dati utili per un confronto con gli anni precedenti.

Le rilevazioni hanno riguardato i flussi documentali in entrata e in uscita, suddivisi per singole unità organizzative. Il raffronto poi con le risorse umane impiegate, le ore effettive lavorate a fronte delle ore teoriche, ha permesso di avere un quadro complessivo delle attività lavorative e la situazione per singole unità organizzative. In tale maniera si sono poste le basi per un sistema di valutazione dei flussi documentali in entrata e uscita e delle risorse necessarie per definire le pratiche in arrivo e smaltire l'arretrato accumulatosi.

Per fornire un monitoraggio costante, nel breve e nel lungo periodo, le rilevazioni sono molteplici, con cadenza mensile, trimestrale, semestrale ed annuale. Sono stati in particolare evidenziati i settori con maggiore quantità di affari da trattare, per indicare i profili più rilevanti ed eventuali criticità.

I rapporti prodotti sono corredati da grafici e note esplicative che agevolano la percezione dei fenomeni evidenziati nelle tabelle. Ulteriori grafici esplicativi sono stati elaborati per rendere maggiormente evidenti e immediate le rilevazioni effettuate, tenendo conto dei suggerimenti forniti dalle unità organizzative.

Il consolidamento delle rilevazioni e delle analisi dei dati dei rapporti prodotti ha permesso di costituire una buona base di confronto fra i periodi pregressi e quello attuale, in maniera da analizzare il trend, in vista dell'adozione degli opportuni accorgimenti per l'equilibrio dei carichi di lavoro tra unità organizzative.

Quella che era una rilevazione straordinaria relativa alla ricognizione dei fascicoli relativi a pratiche arretrate in attesa di essere definiti è diventata una costante e le singole unità organizzative hanno ora un utile strumento per monitorare le pratiche da evadere.

Al contempo si è consolidata anche l'attività di elaborazione di indicatori di efficienza-efficacia, relativi al rapporto tra pratiche definite ed effettive risorse disponibili.

Il gruppo di lavoro sulle problematiche emergenti dall'attuale sistema di protocollazione ha terminato i lavori e preso visione delle caratteristiche di alcuni *software* in commercio, per sostituire l'attuale sistema di protocollazione, ormai datato, che non permette di seguire adeguatamente il flusso documentale in entrata e in uscita e i relativi passaggi intermedi. In questo modo si potrebbe anche affinare i rapporti per perseguire una maggiore efficacia nell'analisi dei flussi documentali.

Sono stati elaborati progetti relativi ad indagini di *customer satisfaction* e alla predisposizione di un sistema gestionale strutturato per centri di costo e centri di responsabilità.

21. DATI STATISTICI (*)

1. Sintesi delle principali attività dell'Autorità

SINTESI DELLE PRINCIPALI ATTIVITÀ DELL'AUTORITÀ	
Numero complessivo dei provvedimenti collegiali adottati	538
Ricorsi decisi (art. 145 del Codice)	257
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154 del Codice)	32
Altri provvedimenti collegiali	249
Notificazioni pervenute nell'anno 2011	1.218
Notificazioni pervenute dal 2004 al 31 dicembre 2011	19.974
Violazioni amministrative contestate	358
Sanzioni applicate con ordinanza di ingiunzione	174
Violazioni penali segnalate all'autorità giudiziaria	37
Riscontri a segnalazioni e reclami	3.223
Risposte a quesiti	387
Ricorsi (trattati) *ex* art. 152 del Codice	170
Opposizioni (trattate) a provvedimenti del Garante	72
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	447
Altre richieste ai sensi dell'art. 157 del Codice non effettuate direttamente presso i titolari	139
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	12
Provvedimenti su verifiche preliminari per trattamenti che presentano rischi specifici	22
Comunicazioni al Garante su flussi di dati tra p.a. o in temi di ricerca	15
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	6
Risposte ad atti di sindacato ispettivo e di controllo	4
Leggi regionali esaminate (di cui con rilievi ai fini dell'impugnazione *ex* art. 127 della Costituzione)	29 (4)
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	31
Riunioni autorità comuni di controllo (Europol, Schengen, Dogane, Eurodac) e del *Wppj - Working party on police and justice*	28
Riunioni presso altri organismi internazionali e *workshop*	19

2. Altre attività dell'Autorità

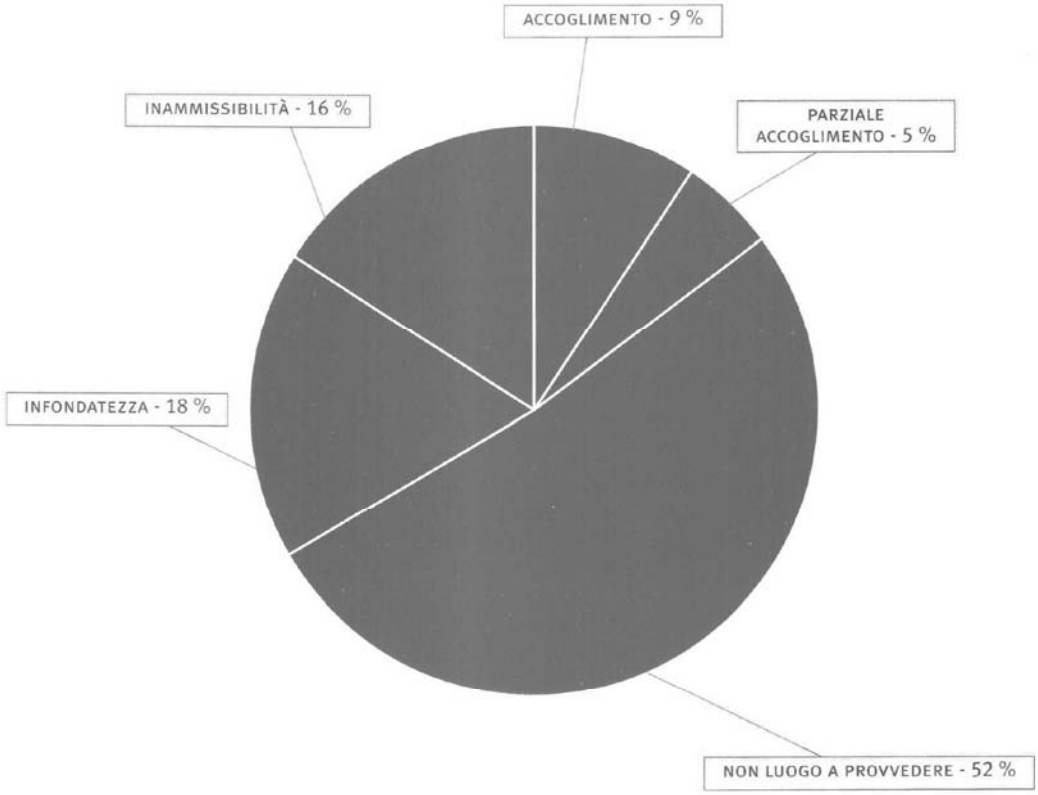
ALTRE ATTIVITÀ DELL'AUTORITÀ	
Comunicati stampa	35
Newsletter	9
Dvd (edizioni pubblicate)	1
Dépliant	2
Pubblicazioni	4
Conferenze internazionali (1)	2

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2011. Singole note indicano altri periodi o situazioni e casi specifici. I dati delle tabelle 9, 10, 11 si riferiscono ai fascicoli istituiti presso l'Ufficio

(1) Una delle due conferenze è stata organizzata congiuntamente dal Servizio relazioni internazionali e dal Servizio relazioni mezzi informazione

3. Tipologia delle decisioni su ricorsi (tabella e grafico)

DECISIONI SU RICORSI	
TIPI DI DECISIONE (1)	NUMERO RICORSI
Accoglimento	24
Parziale accoglimento	14
Non luogo a provvedere (2)	133
Infondatezza	45
Inammissibilità	41
Totale	257

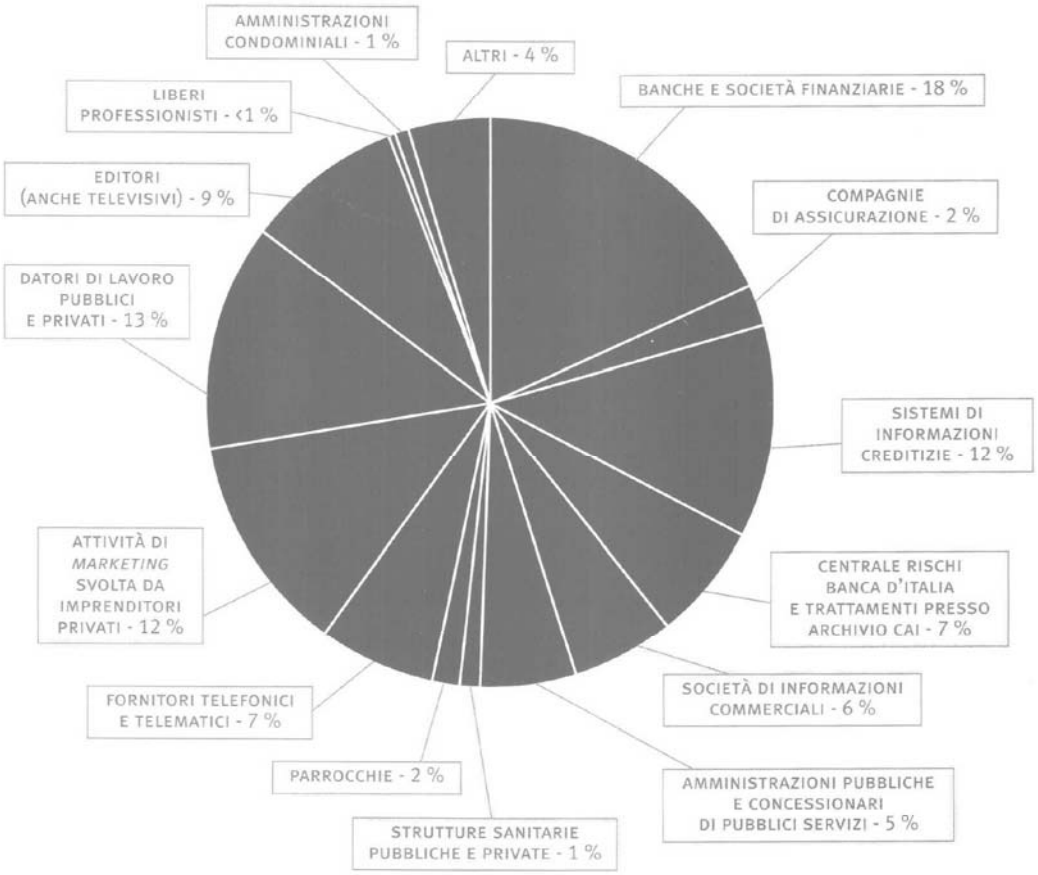


(1) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole"

(2) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

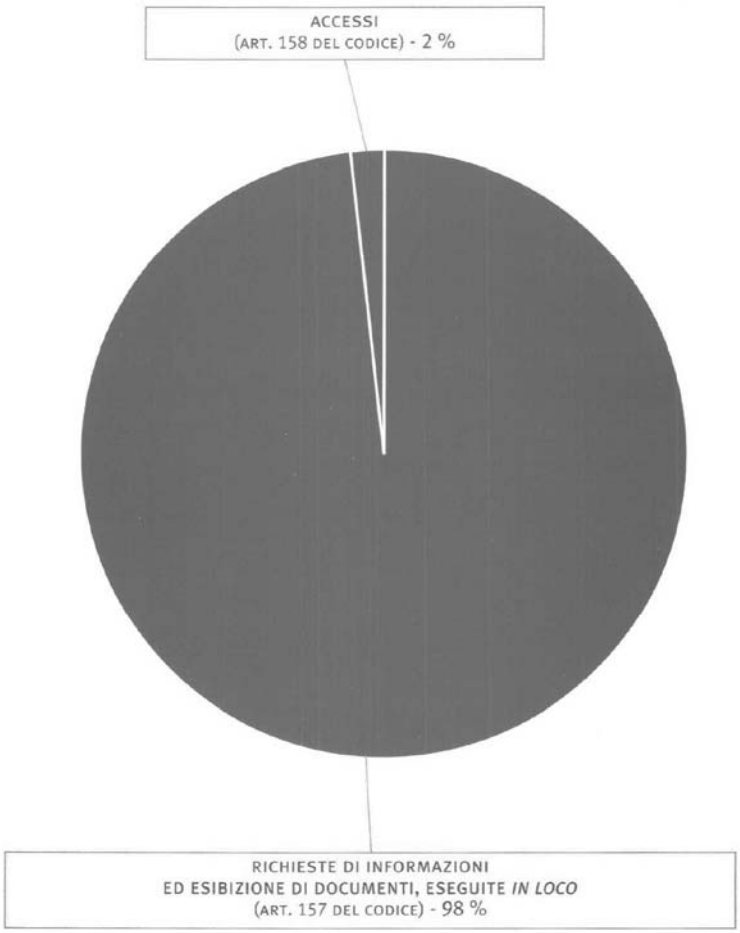
CATEGORIA DI TITOLARI	NUMERO RICORSI
Banche e società finanziarie	47
Compagnie di assicurazione	6
Sistemi di informazioni creditizie	31
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	17
Società di informazioni commerciali	15
Amministrazioni pubbliche e concessionari di pubblici servizi	14
Strutture sanitarie pubbliche e private	3
Parrocchie	4
Fornitori telefonici e telematici	17
Attività di *marketing* svolta da imprenditori privati	32
Datori di lavoro pubblici e privati	33
Editori (anche televisivi)	23
Liberi professionisti	1
Amministrazioni condominiali	2
Altri	12
Totale	**257**

4. Suddivisione dei ricorsi in relazione alla categoria di titolari del trattamento (tabella e grafico)



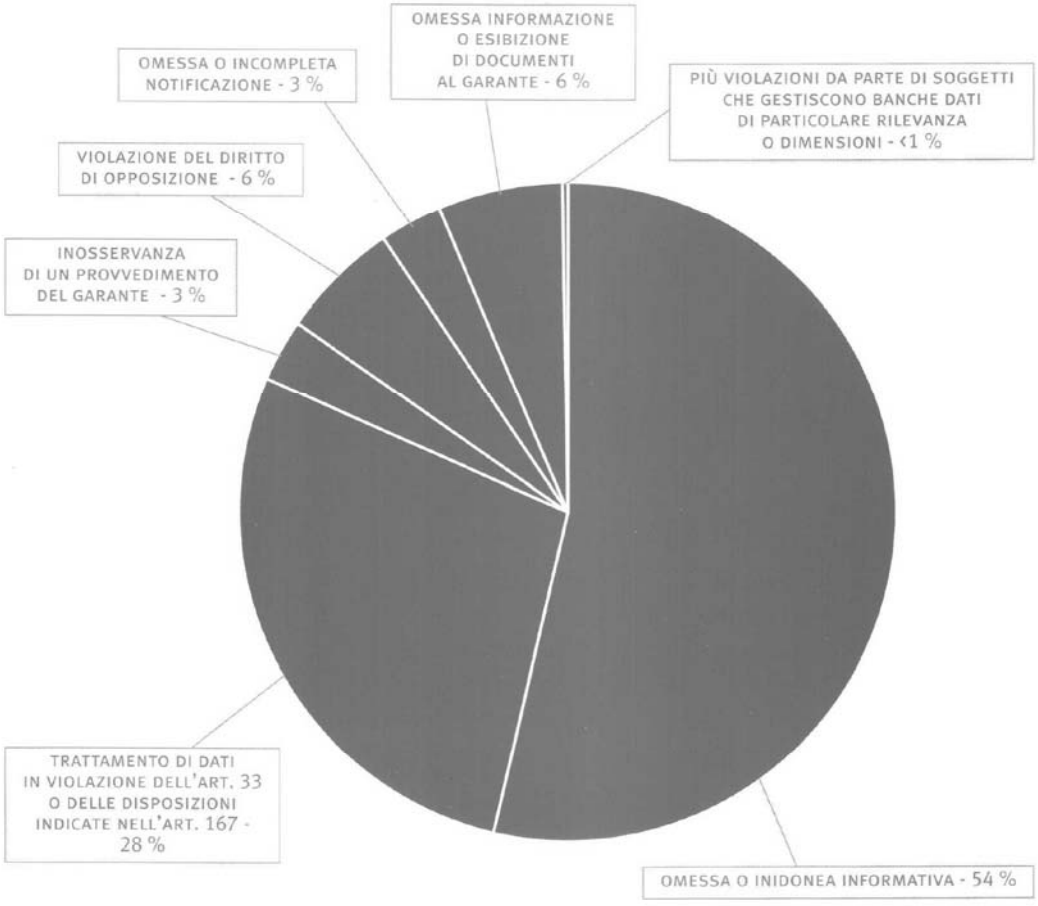
5. Accertamenti e controlli eseguiti (tabella e grafico)

ACCERTAMENTI E CONTROLLI ESEGUITI DIRETTAMENTE PRESSO TITOLARI DEL TRATTAMENTO	
Richieste di informazioni ed esibizione di documenti, eseguite *in loco* (art. 157 del Codice)	439
Accessi (art. 158 del Codice)	8
Totale	447



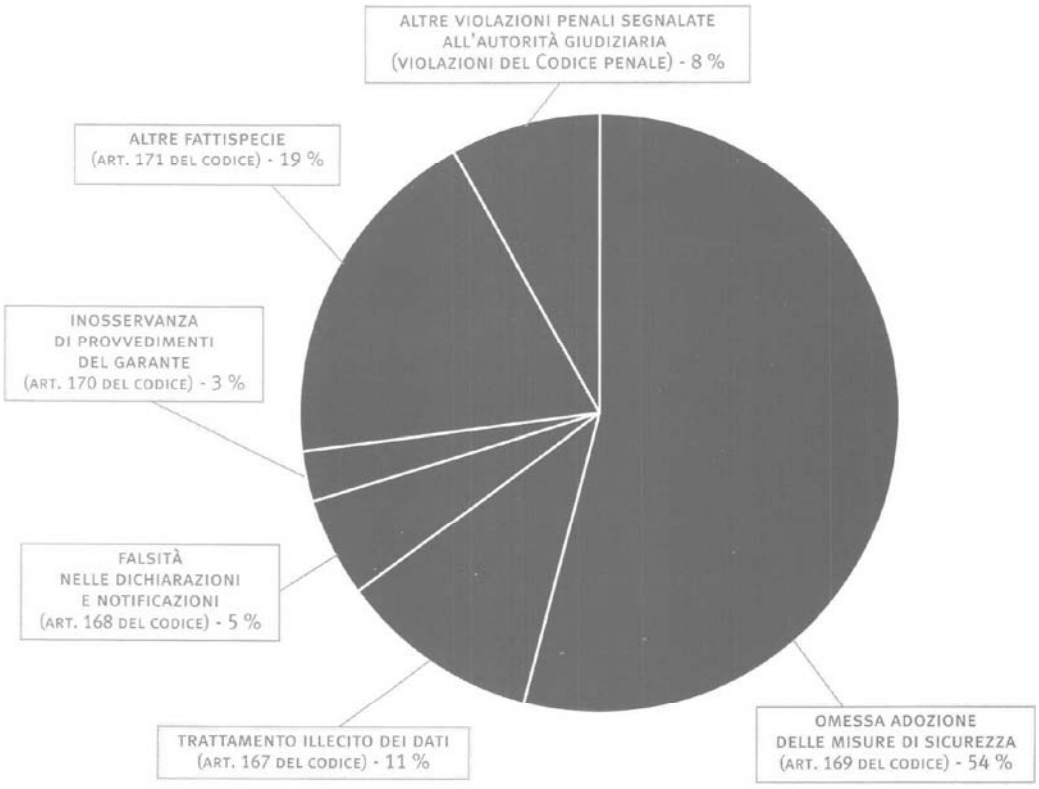
VIOLAZIONI AMMINISTRATIVE CONTESTATE	
Omessa o inidonea informativa (art. 161 del Codice)	192
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	100
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	11
Violazione del diritto di opposizione (art. 162, comma 2-*quater*, del Codice)	21
Omessa o incompleta notificazione (art. 163 del Codice)	11
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	22
Più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	1
Totale	**358**

6. Violazioni amministrative contestate (tabella e grafico)



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)	20
Trattamento illecito dei dati (art. 167 del Codice)	4
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	2
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	1
Altre fattispecie (art. 171 del Codice)	7
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del Codice penale)	3
Totale	37



8. Pagamenti derivanti dall'attività sanzionatoria

PAGAMENTI DERIVANTI DALL'ATTIVITÀ SANZIONATORIA	
Somme versate a titolo di oblazione in via breve	1.810.400
Somme versate in conseguenza di ordinanze ingiunzione	830.530
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	432.500
Totale	**3.073.430**

9. Pareri (ex art. 154, comma 4, del Codice)

PARERI (EX ART. 154, COMMA 4, DEL CODICE)	
TEMI	RISCONTRI RESI NELL'ANNO (1)
Attività di polizia, sicurezza nazionale e governo del territorio	2
Giustizia	2
Informatizzazione e banche dati della p.a.	8
Formazione	3
Rapporto di lavoro pubblico	2
Tutela della salute e attività sanitaria	6
Attività produttive e professioni	5
Solidarietà sociale	2
Stato civile e anagrafe	2
Totale	32

10. Quesiti

QUESITI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	332	387

11. Segnalazioni e reclami

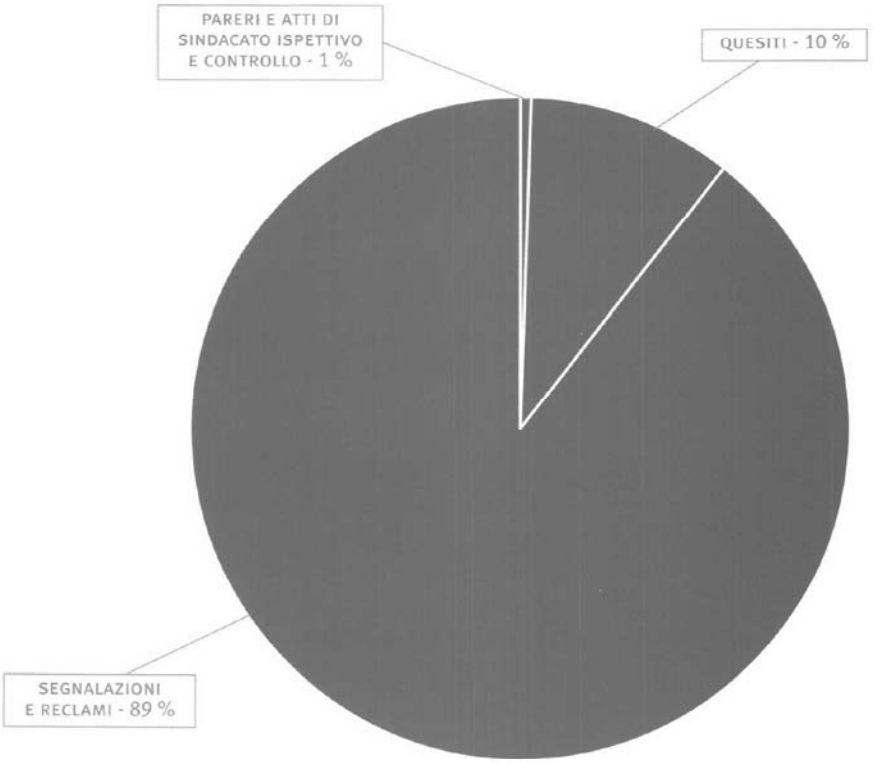
SEGNALAZIONI E RECLAMI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
Totale	4.022	3.223
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	-	11
Assicurazioni	92	71
Associazioni	43	23
Centrali rischi	203	200
Concessionari pubblici servizi	127	142
Condominio	43	25
Credito	250	262
Dati dei dipendenti e fascicoli personali	12	118
Enti locali	36	36
Giornalismo e libertà d'espressione	220	168
Giustizia e accertamenti di polizia	4	22
Imprese	127	98
Informazioni commerciali	8	3
Internet e informatizzazione	19	84
Lavoro	247	168
Marketing	21	20
Pubblicità non gradita	3	12
Recupero crediti	111	122
Rilevazioni biometriche	4	9
Sanità e servizi di assistenza sociale	24	54
Telefonia	1.918	1.258
Trasparenza	-	5
Tributi	6	10
Videosorveglianza	202	234

(1) Inerenti anche ad affari pervenuti anteriormente al 2011

12. Atti di sindacato ispettivo e controllo

ATTI DI SINDACATO ISPETTIVO E CONTROLLO	
TEMI	NUMERO
Trattamento di dati sensibili mediante *test* per la selezione di personale	1
Acquisizione indebita di immagini o intercettazioni	1
Tutela nei confronti dei *social networks*	1
Registro pubblico delle opposizioni	1
Totale	4

Grafico delle tipologie dei riscontri resi a interessati e richiedenti



13. Tipologie di notificazioni pervenute nel 2011

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL 2011 (1)			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	30	802	832
Modifica di una precedente notificazione	21	287	308
Notificazione della cessazione del trattamento	7	71	78
Totale	58	1.160	1.218

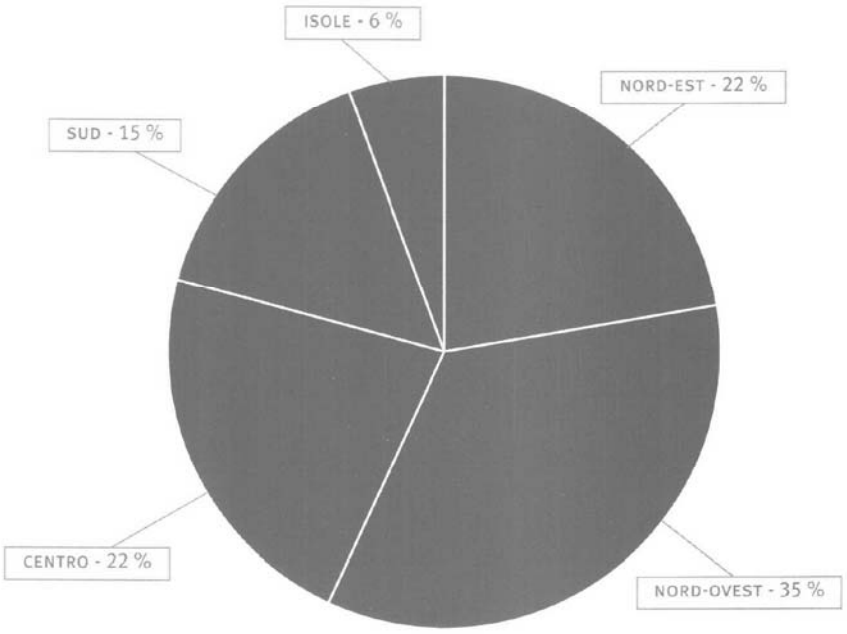
(1) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2011

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL PERIODO 2004-2011			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	1.125	15.553	16.678
Modifica di una precedente notificazione	107	2.592	2.699
Notificazione della cessazione del trattamento	61	536	597
Totale	1.293	18.681	19.974

14. Tipologie di notificazioni pervenute nel periodo 2004-2011

PROVENIENZA GEOGRAFICA DELLE NOTIFICAZIONI: 2004-2011	
ITALIA	
ZONE GEOGRAFICHE	PERVENUTE
Nord-Est	4.443
Nord-Ovest	6.863
Centro	4.423
Sud	3.033
Isole	1.116
Totale	19.878
Da altri Paesi	96

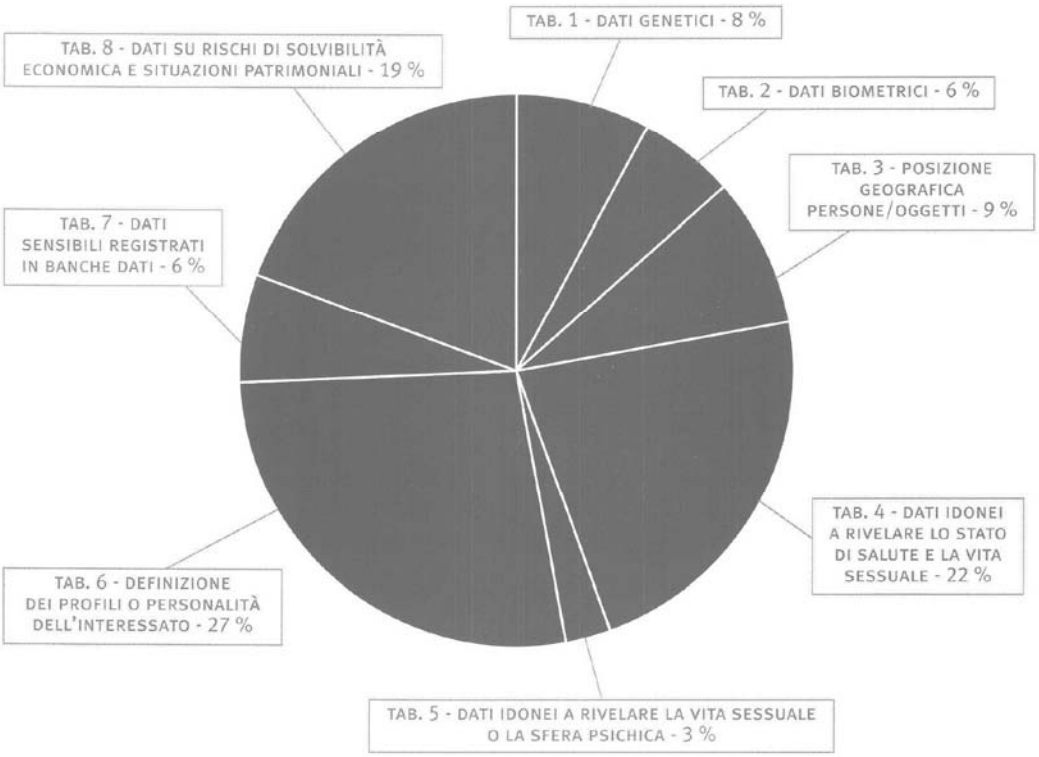
15. Provenienza geografica delle notificazioni: 2004-2011 (tabella e grafico)



(1) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2011

16. Suddivisione delle notificazioni per tipologia di trattamento svolto 2004-2011 (tabella e grafico)

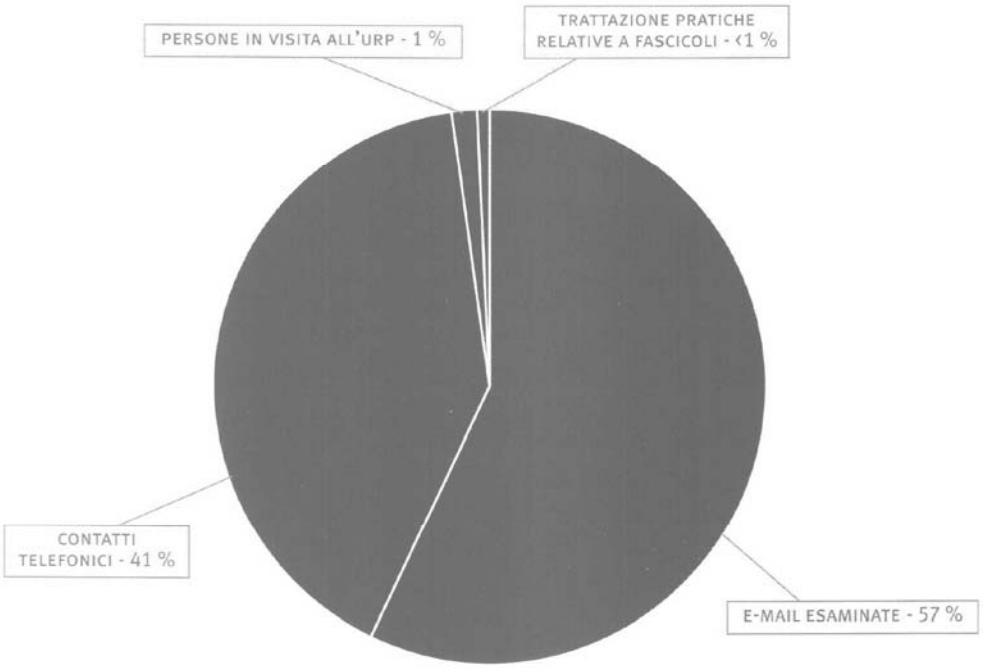
SUDDIVISIONE DELLE NOTIFICAZIONI PER TIPOLOGIA DI TRATTAMENTO SVOLTO 2004-2011	
TABELLE DI NOTIFICAZIONE COMPILATE (1)	NUMERO
Tabella 1 - Trattamento di dati genetici	2.311
Tabella 2 - Trattamento di dati biometrici	1.662
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	2.568
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	6.587
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	781
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	8.031
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	1.866
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	5.718
Totale	**29.524**



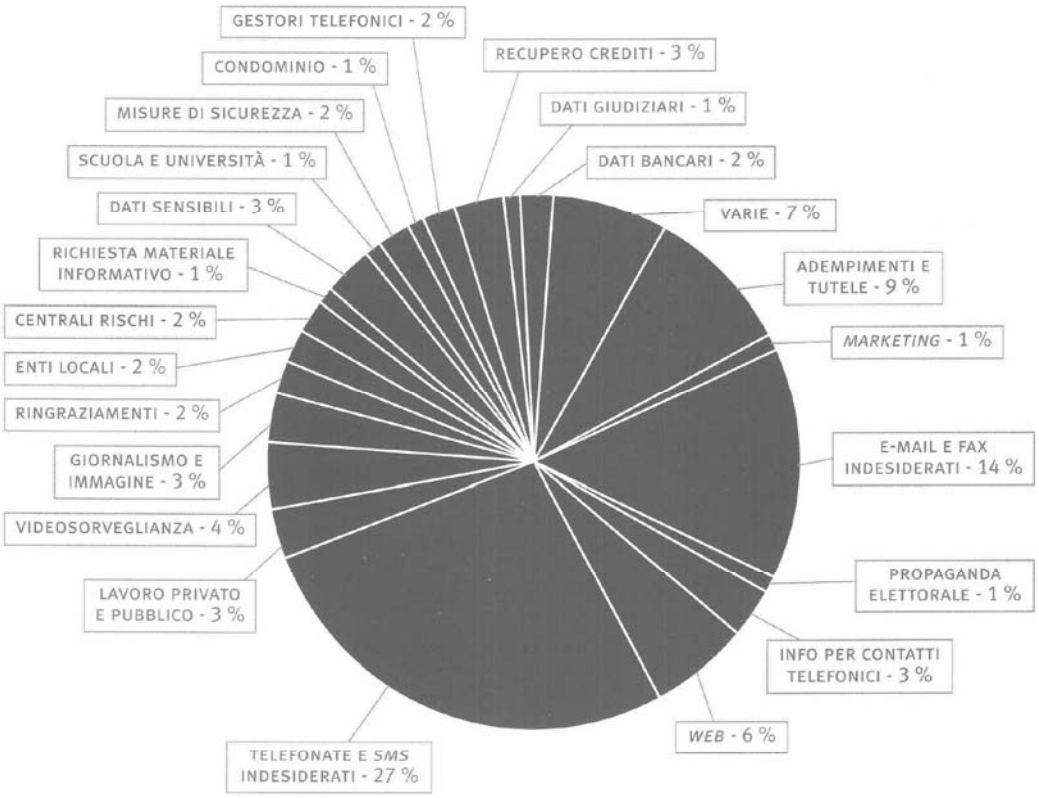
(1) Situazione alla data del 31 dicembre 2011

UFFICIO RELAZIONI CON IL PUBBLICO	
	2011
E-mail esaminate	18.214
Contatti telefonici	13.000
Persone in visita all'URP	472
Trattazione pratiche relative a fascicoli	235
Totale	31.921

17. Ufficio relazioni con il pubblico (tabella e grafico)



18. E-mail esaminate dall'Ufficio relazioni con il pubblico [grafico delle categorie]



19. Posti previsti in organico

POSTI PREVISTI IN ORGANICO	
Segretario generale	1
Dirigenti	24
Funzionari	69
Operativi	30
Esecutivi	1
Totale	**125**
Personale a contratto	20

20. Personale in servizio

PERSONALE IN SERVIZIO (1)				
AREA	IN RUOLO (A)	IN POSIZIONE DI FUORI RUOLO (B)	COMANDATO PRESSO ALTRE AMMINISTRAZIONI O IN ASPETTATIVA (C)	IMPIEGATO DALL'UFFICIO (A+B-C)
Segretario generale	1			1
Dirigenti	15	3	1	17
Funzionari	59	5	5	59
Operativi	24	2		26
Esecutivi				0
Totale	**99**	**10**	**6**	**103**
Personale a contratto				20

21. Risorse finanziarie

RISORSE FINANZIARIE						
ENTRATE ACCERTATE	ANNO 2011		ANNO 2010		DIFFERENZA	
Correnti		23.779.047		16.606.197		7.172.850
di cui trasferimento dallo Stato	8.532.693		13.373.059		-4.840.366	
Totale entrate		**23.779.047**		**16.606.197**		**7.172.850**
SPESE IMPEGNATE	ANNO 2011		ANNO 2010		DIFFERENZA	
Funzionamento		18.542.326		17.616.735		925.591
Capitale		420.528		114.742		305.786
Rimborsi al MEF		251.735		-		251.735
Totale spese		**19.214.589**		**17.731.477**		**1.483.112**

(1) Situazione alla data del 31 dicembre 2011

Documentazione

IV. Documentazione

22. Provvedimenti del Garante

Prescrizioni all'Istat sulle modalità di pubblicazione dell'informativa sul trattamento di dati personali nell'ambito del 15° Censimento generale della popolazione e delle abitazioni
19 gennaio 2011 [doc. *web* n. 1784974]

Prescrizioni per il trattamento di dati personali per finalità di *marketing*, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del Registro pubblico delle opposizioni
19 gennaio 2011 [doc. *web* n. 1784528]

Prenotazioni e ritiro analisi in farmacia: via libera del Garante *privacy*
19 gennaio 2011 [doc. *web* n. 1787887]

Scambio di informazioni tra i Ministeri dell'interno e delle infrastrutture e dei trasporti ai fini del rilascio e della revoca dei titoli abilitativi alla guida di veicoli, motoveicoli e ciclomotori
26 gennaio 2011 [doc. *web* n. 1790365]

Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso il Principato di Andorra
3 febbraio 2011 [doc. *web* n. 1788981]

Fondo per il diritto al lavoro dei disabili e trattamento di dati sensibili
3 febbraio 2011 [doc. *web* n. 1790408]

Customer care: garanzie per il trattamento dei dati personali degli utenti e dei lavoratori di *call center*
9 febbraio 2011 [doc. *web* n. 1797032]

CONI: registro delle sanzioni disciplinari e trattamento di dati personali

16 febbraio 2011 [doc. *web* n. 1793469]

Privacy più tutelata per i disabili che acquistano un'autovettura

16 febbraio 2011 [doc. *web* n. 1792975]

Caricamento di dati sanitari di emergenza nella tessera personale di riconoscimento del personale militare: misure per garantire la *privacy* degli interessati

16 febbraio 2011 [doc. *web* n. 1797055]

Ordinanza di ingiunzione per illegittimo trattamento di dati personali

16 febbraio 2011 [doc. *web* n. 1855692]

10 giugno 2011 [doc. *web* n. 1859107]

Documenti contenenti dati personali idonei a rivelare lo stato di salute: la consegna deve avvenire in busta chiusa

24 febbraio 2011 [doc. *web* n. 1797075]

Modelli di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati ai servizi di telefonia fissa e mobile

24 febbraio 2011 [doc. *web* n. 1794638]

Lavoro: garanzie per il trattamento e la comunicazione di dati personali dei dipendenti

2 marzo 2011 [doc. *web* n. 1802433]

Fax promozionali: illeciti senza consenso

2 marzo 2011 [doc. *web* n. 1802423]

Trattamento sproporzionato di dati biometrici dei dipendenti per finalità di accesso alla sede aziendale

10 marzo 2011 [doc. *web* n. 1807683]

Richiesta di cancellazione da archivio *online* di dati personali

23 marzo 2011 [doc. *web* n. 1807050]

21 dicembre 2011 [doc. *web* n. 1877115]

Esonero dall'obbligo di rendere l'informativa per un sistema di raccolta e organizzazione di informazioni pubbliche presenti su internet e concernenti il mercato dell'energia

31 marzo 2011 [doc. *web* n. 1810147]

Cessazione dell'efficacia del provvedimento di divieto adottato il 24 febbraio 2010

31 marzo 2011 [doc. *web* n. 1807758]

In assenza di consenso specifico e informato, illecito il trattamento di dati personali di minori disabili per l'invio di comunicazioni promozionali

31 marzo 2011 [doc. *web* n. 1810166]

Vietato il trattamento di dati personali del dipendente ricavati da file e documenti acquisiti nell'ambito di operazioni di *backup* effettuate sul *server* aziendale

7 aprile 2011 [doc. *web* n. 1812154]

Propaganda elettorale: le regole del Garante *privacy*

7 aprile 2011 [doc. *web* n. 1804225]

Invio di comunicazioni promozionali con modalità automatizzate, senza consenso e senza idonea informativa

7 aprile 2011 [doc. *web* n. 1810207]

5 maggio 2011 [doc. *web* n. 1822815]

10 giugno 2011 [doc. *web* n. 1836396]

30 giugno 2011 [doc. *web* n. 1834208]

26 ottobre 2011 [doc. *web* n. 1851750]

24 novembre 2011 [doc. *web* n. 1876435]

Elenchi telefonici *online*: illegittimi se la fonte dei dati non è il DBU

7 aprile 2011 [doc. *web* n. 1810351]

Stop a "fax selvaggio"

7 aprile 2011 [doc. *web* n. 1810207]

Preiscrizioni universitarie per l'anno accademico 2011/2012

7 aprile 2011 [doc. *web* n. 1807556]

Prescrizioni per il corretto impiego di un sistema di videosorveglianza all'interno di un hotel

14 aprile 2011 [doc. *web* n. 1810223]

Convenzione fra la Direzione investigativa antimafia e l'Inail per l'accesso alla banca dati relativa ai documenti unici di regolarità contributiva

14 aprile 2011 [doc. *web* n. 1813942]

Digit-PA: regole tecniche per la consultazione ed estrazione di indirizzi e di elenchi di indirizzi di posta elettronica certificata (PEC) di cittadini, imprese e professionisti, da parte della pubblica amministrazione

21 aprile 2011 [doc. *web* n. 1807547]

Disposizioni in materia di stato civile relativamente alla disciplina sul cognome

27 aprile 2011 [doc. *web* n. 1816423]

Internet: ordinanze di custodia cautelare e garanzie per gli interessati

5 maggio 2011 [doc. *web* n. 1827129]

Trasferimento di dati personali all'estero - Autorizzazione alla Società per Azioni Michelin Italiana

5 maggio 2011 [doc. *web* n. 1829762]

Linee-guida in tema di trattamento di dati per lo svolgimento di indagini di *customer satisfaction* in ambito sanitario

5 maggio 2011 [doc. *web* n. 1812910]

Proroga dei termini per l'adempimento delle prescrizioni di cui alla lettera a) del provvedimento del 24 febbraio 2011 recante "modelli di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati ai servizi di telefonia fissa e mobile"

5 maggio 2011 [doc. *web* n. 1811916]

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

12 maggio 2011 [doc. *web* n. 1813953]

Parere del Garante su uno schema di decreto del Presidente della Repubblica recante "Regolamento di attuazione in materia di risoluzione del rapporto di lavoro dei dipendenti delle amministrazioni pubbliche dello Stato e degli enti pubblici nazionali in caso di permanente inidoneità psicofisica"

19 maggio 2011 [doc. *web* n. 1890453]

Rilevazione di dati biometrici dei dipendenti - verifica preliminare

26 maggio 2011 [doc. *web* n. 1832558]

10 giugno 2011 [doc. *web* n. 1835792]

Convenzione fra il Ministero dell'interno-Dipartimento della pubblica sicurezza e l'Agenzia delle entrate per l'accesso da parte delle forze di polizia alla banca dati dell'Anagrafe tributaria attraverso l'applicativo denominato "Puntofisco"
26 maggio 2011 [doc. *web* n. 1822278]

Camere di commercio: più tutele nella designazione dei consiglieri
26 maggio 2011 [doc. *web* n. 1817531]

Parere del Garante al Ministero dello sviluppo economico sullo schema di decreto recante "Regolamento relativo alla designazione e nomina dei componenti del consiglio ed all'elezione dei membri della giunta delle Camere di commercio, industria, artigianato e agricoltura"
26 maggio 2011 [doc. *web* n. 1890457]

Regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione
10 giugno 2011 [doc. *web* n. 1822296]

Documento progettuale per la produzione, il rilascio e la gestione del modello ATe da parte delle amministrazioni dello Stato
10 giugno 2011 [doc. *web* n. 1822311]

Accesso dell'interessato a dati personali riguardanti la gestione del rapporto di lavoro
15 giugno 2011 [doc. *web* n. 1829925]
15 giugno 2011 [doc. *web* n. 1827162]
15 dicembre 2011 [doc. *web* n. 1876777]

Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali
15 giugno 2011 [doc. *web* n. 1821257]

Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione
15 giugno 2011 [doc. *web* n. 1826687]

Autorizzazione n. 2/2011 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale
24 giugno 2011 [doc. *web* n. 1822577]

Autorizzazione n. 4/2011 al trattamento dei dati sensibili da parte dei liberi professionisti
24 giugno 2011 [doc. *web* n. 1822597]

Autorizzazione n. 6/2011 al trattamento dei dati sensibili da parte degli investigatori privati
24 giugno 2011 [doc. *web* n. 1822629]

Nuovo regolamento di gestione dell'INA
24 giugno 2011 [doc. *web* n. 1826698]

Autorizzazione generale al trattamento dei dati genetici
24 giugno 2011 [doc. *web* n. 1822650]

Esonero dall'obbligo di notificazione del trattamento di dati genetici effettuato da organismi di mediazione
24 giugno 2011 [doc. *web* n. 1823225]

Allungamento dei tempi di conservazione delle immagini registrate da un impianto di videosorveglianza. Verifica preliminare
7 luglio 2011 [doc. *web* n. 1836347]
14 luglio 2011 [doc. *web* n. 1836335]

Localizzazione dei veicoli aziendali a prova di *privacy*. Verifica preliminare
7 luglio 2011 [doc. *web* n. 1828371]
7 luglio 2011 [doc. *web* n. 1828354]

Prescrizioni relative all'implementazione del provvedimento del 1° aprile 2010 in materia di trattamento dei dati personali degli abbonati ai servizi di telefonia fissa e mobile in caso di *number portability*
7 luglio 2011 [doc. *web* n. 1824538]

Sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp) e regole per il trattamento dei dati
7 luglio 2011 [doc. *web* n. 1829704]

Linee-guida dei siti *web* delle pubbliche amministrazioni del Ministro per la pubblica amministrazione e l'innovazione
7 luglio 2011 [doc. *web* n. 1826713]

Schema di decreto ministeriale riguardante le modalità e i contenuti della prova di ammissione al corso di laurea magistrale in medicina e chirurgia attivato in lingua inglese presso gli Atenei di Milano, di Pavia e di Roma "La Sapienza" per l'anno accademico 2011/2012
7 luglio 2011 [doc. *web* n. 1826705]

Richiesta di cancellazione da un sito *web* di dati relativi allo svolgimento di attività politica
7 luglio 2011 [doc. *web* n. 1834934

Bozza di ordinanza del Presidente del Consiglio dei ministri, recante "Ulteriori disposizioni urgenti dirette a fronteggiare lo stato di emergenza umanitaria nel territorio nazionale in relazione all'eccezionale afflusso di cittadini appartenenti ai paesi del Nord Africa"
14 luglio 2011 [doc. *web* n. 1826722]

Illecito il questionario per la selezione del personale

21 luglio 2011 [doc. *web* n. 1825852]

Il Garante *privacy* al Poligrafico: più tutele per i lavoratori

21 luglio 2011 [doc. *web* n. 1829641]

Autorizzazione al trattamento di dati di pazienti per uno studio osservazionale senza consenso informato

21 luglio 2011 [doc. *web* n. 1836317]

15 settembre 2011 [doc. *web* n. 1849964]

1° dicembre 2011 [doc. *web* n. 1872054]

20 gennaio 2012 [doc. *web* n. 1872049]

25 gennaio 2012 [doc. *web* n. 1872084]

Telefonate promozionali con operatore verso soggetti intestatari di un'utenza telefonica riservata

21 luglio 2011 [doc. *web* 1832551]

Enti caritativi e "carta acquisti": ok del Garante alla sperimentazione

27 luglio 2011 [doc. *web* n. 1832767]

Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso le Isole Fær Øer

7 settembre 2011 [doc. *web* n. 1838283]

Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso il Baliato di Jersey

7 settembre 2011 [doc. *web* n. 1838359]

Prescrizioni per il trattamento di dati personali da parte di Unitelma Sapienza Università Telematica

7 settembre 2011 [doc. *web* n. 1844176]

Proroga dei termini per l'adempimento delle prescrizioni di cui al provvedimento del 15 giugno 2011 in materia di titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali
7 settembre 2011 [doc. *web* n. 1839211]

Parere sullo schema di convenzione tra il Centro coordinamento nazionale per la viabilità (Viabilità Italia) e gli operatori dei servizi di comunicazione elettronica, per la fornitura del servizio di invio di messaggi in situazioni di crisi della viabilità nazionale
15 settembre 2011 [doc. *web* n. 1844167]

Servizi a valore aggiunto (VAS): individuazione del titolare del trattamento dei dati personali degli utenti effettuato dal fornitore del servizio e dai gestori telefonici
15 settembre 2011 [doc. *web* n. 1849872]

Autorizzazione al trattamento dei dati di pazienti per uno studio biomedico senza consenso informato
22 settembre 2011 [doc. *web* n. 1849897]
11 ottobre 2011 [doc. *web* n. 1849933]

Giustizia tributaria: concorsi e dati personali
22 settembre 2011 [doc. *web* n. 1844190]

Parere sullo schema di decreto recante "Disposizioni regolamentari in materia di ordinamento militare"
22 settembre 2011 [doc. *web* n. 1844183]

Vietate le telefonate promozionali a fini di *marketing* verso numeri tratti da albi professionali senza il consenso preventivo dell'interessato
29 settembre 2011 [doc. *web* n. 1851415]

Trattamento di dati personali e sensibili nell'ambito del sistema informativo per il monitoraggio dell'assistenza erogata presso gli *hospice*
11 ottobre 2011 [doc. *web* n. 1851388]

Trasferimento di dati personali all'estero - Autorizzazione alla Fondazione Michelin Sviluppo
11 ottobre 2011 [doc. *web* n. 1849957]

Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro
4 ottobre 2011 [doc. *web* n. 1850581]

Parere del Garante sulle modalità di esercizio del diritto di voto per corrispondenza da parte degli elettori iscritti nelle liste elettorali di un comune della Provincia di Bolzano
20 ottobre 2011 [doc. *web* n. 1851426]

Parere su uno schema di linee-guida in materia di *Disaster Recovery* delle pubbliche amministrazioni
20 ottobre 2011 [doc. *web* n. 1851672]

Divieto di trattamento dei dati biometrici dei dipendenti per finalità di rilevazione della presenza sul posto di lavoro
20 ottobre 2011 [doc. *web* n. 1851657]

Parere al Ministero dell'economia e delle finanze sulle linee di indirizzo in materia di misure regionali di compartecipazione alla spesa sanitaria per fasce di reddito
26 ottobre 2011 [doc. *web* n. 1851679]

Impiego di sistemi di videosorveglianza
10 novembre 2011 [doc. *web* n. 1859539]
10 novembre 2011 [doc. *web* n. 1859569]

17 novembre 2011 [doc. *web* n. 1859558]

17 novembre 2011 [doc. *web* n. 1859546]

Parere al Ministero dell'economia e delle finanze su uno schema di regolamento di concerto con il Ministro della giustizia riguardante il tirocinio per l'esercizio dell'attività di revisione legale
10 novembre 2011 [doc. *web* n. 1851797]

Parere al Ministero dell'economia e delle finanze su uno schema di regolamento di concerto con il Ministro della giustizia concernente il contenuto e le modalità di iscrizione nonché i casi e le modalità di cancellazione dal registro dei revisori legali
10 novembre 2011 [doc. *web* n. 1851772]

Parere al Ministero dell'economia e delle finanze su uno schema di regolamento concernente i requisiti per l'iscrizione al registro dei revisori legali
10 novembre 2011 [doc. *web* n. 1851757]

Parere su uno schema di decreto del Presidente del Consiglio dei ministri in materia di separati certificati di firma
24 novembre 2011 [doc. *web* n. 1870611]

Parere su uno schema di decreto del Presidente del Consiglio dei ministri recante regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
24 novembre 2011 [doc. *web* n. 1870620]

Parere su uno schema di decreto del Presidente del Consiglio dei ministri recante regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata
24 novembre 2011 [doc. *web* n. 1870629]

Trascrizione di un'intercettazione telefonica relativa ad un colloquio fra un noto esponente politico e un dirigente della RAI
24 novembre 2011 [doc. *web* n. 1870903]

Incompatibilità nel rapporto di pubblico impiego: comunicazione di dati personali tra l'Inps e un'azienda ospedaliera
24 novembre 2011 [doc. *web* n. 1880524]

Decisione di non luogo a provvedere, per intervenuta comunicazione dei dati richiesti dall'interessato
6 dicembre 2011 [doc. *web* n. 1872740]

Trattamento di dati sensibili attinenti alla vita sessuale
6 dicembre 2011 [doc. *web* n. 1872753]

Parere del Garante su uno schema di regolamento riguardante dati e operazioni che il Ministero dell'economia e delle finanze è autorizzato a trattare ed effettuare in applicazione della normativa sul funzionamento dei registri dei revisori legali e dei tirocinanti
15 dicembre 2011 [doc. *web* n. 1882020]

Società interessate da un'operazione di fusione per incorporazione: prescrizioni per l'informativa da rendere agli interessati
1 dicembre 2011 [doc. *web* n. 1872641]

Prescrizioni del Garante per le chiamate a carattere commerciale cd. "mute"
6 dicembre 2011 [doc. *web* n. 1857326]

Modifica del provvedimento 14 maggio 2009, recante esonero dall'informativa per l'Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito (Ancic)
15 dicembre 2011 [doc. *web* n. 1862497]

Ricevitorie e tabaccherie Sisal: garanzie per la raccolta e il trattamento dei dati
15 dicembre 2011 [doc. *web* n. 1883880]

Consultazione pubblica sul documento recante lo schema di autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute per studi osservazionali retrospettivi
15 dicembre 2011 [doc. *web* n. 1859602]

Parere al Ministero della giustizia in tema di regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione
21 dicembre 2011 [doc. *web* n. 1870802]

Parere del Garante in ordine a uno schema di ordinanza di necessità e urgenza del Ministro, relativa all'adozione di provvedimenti in materia di protesi mammarie cosiddette PIP
29 dicembre 2011 [doc. *web* n. 1863619]

Trattamento di dati in occasione di riprese televisive riguardanti una vicenda di rilevante interesse pubblico
30 dicembre 2011 [doc. *web* n. 1873945]

Lavoro e previdenza sociale. Informativa negli annunci relativi ad offerte di lavoro
10 gennaio 2002 [doc *web* n. 1064553]

Raccolta e utilizzo di dati personali mediante moduli contrattuali senza consenso specifico per ciascuna finalità di trattamento
12 gennaio 2012 [doc. *web* n. 1884254]

Parere alla Presidenza del Consiglio dei ministri-Dipartimento per la pubblica amministrazione e la semplificazione su uno schema di decreto recante regolamento per la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del Sistema Pubblico di connettività (SPC)
12 gennaio 2012 [doc. *web* n. 1872045]

Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso lo Stato d'Israele
20 gennaio 2012 [doc. *web* n. 1868817]

Parere a Unioncamere in ordine alla modifica della scheda relativa al trattamento di dati sensibili e giudiziari effettuato per la gestione e il rinnovo dei componenti degli organi collegiali di amministrazione e controllo
20 gennaio 2012 [doc. *web* n.1870229]

Vietato l'utilizzo di dati personali per finalità di comunicazioni promozionali in assenza del prescritto riscontro presso il Registro pubblico delle opposizioni e tramite chiamate prive dell'identificazione della linea chiamante
23 febbraio 2012 [doc. *web* n. 1877080]
23 febbraio 2012 [doc. *web* n. 1878559]
23 febbraio 2012 [doc. *web* n. 1877065]

Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica
1° marzo 2012 [doc. *web* n. 1878276]

Parere del Garante su uno schema di ordinanza di necessità e urgenza del Ministero della salute per l'adozione di provvedimenti in materia di protesi mammarie cosiddette PIP
1° marzo 2012 [doc. *web* n. 1881229]

Essenzialità dell'informazione riguardo a fatti di pubblico e attuale interesse
8 marzo 2012 [doc. *web* 1887094]

23. PRINCIPALI ATTIVITÀ INTERNAZIONALI

23.1. UNIONE EUROPEA

SISTEMA EUROPEO DI CONTROLLO IN MATERIA DI DATI FINANZIARI

Comunicazione COM(2011) 429 - Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni Sistema europeo di controllo delle transazioni finanziarie dei terroristi: opzioni possibili
13 luglio 2011 [doc. *web* n. 1895709]

REVISIONE DELLA DIRETTIVA N. 95/46/CE

Comunicazione COM(2012) 10 - Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati
25 gennaio 2012 [doc. *web* n. 1895615]

Comunicazione COM(2012) 11 - Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)
25 gennaio 2012 [doc. *web* n. 1895611]

23.2. GRUPPO ART. 29

WP 180 - Parere 9/2011 sulla proposta rivista dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID
11 febbraio 2011 [doc. *web* n. 1895642]

WP 181 - Parere 10/2011 sulla proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi
5 aprile 2011 [doc. *web* n. 1895633]

WP 182 - Parere 11/2011 sul livello di protezione dei dati personali in Nuova Zelanda
4 aprile 2011 [doc. *web* n. 1895715]

WP 183 - Parere 12/2011 sui contatori intelligenti (*smart metering*)
4 aprile 2011 [doc. *web* n. 1895719]

WP 184 - Documento di lavoro 01/2011 sull'attuale quadro nell'UE in materia di violazioni dei dati e raccomandazioni relative alla definizione di future politiche in materia
5 aprile 2011 [doc. *web* n. 1895723]

WP 185 - Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti
16 maggio 2011 [doc. *web* n. 1895727]

WP 186 - Parere 14/2011 sulle questioni di protezione dei dati legate alla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo
13 giugno 2011 [doc. *web* nn. 1895731 e Allegato 1895751]

WP 187 - Parere 15/2011 sulla definizione di consenso
13 luglio 2011 [doc. *web* n. 1895739]

WP 188 - Parere 16/2011 relativo alla raccomandazione dell'EASA/IAB sulle buone prassi in materia di pubblicità comportamentale *online*
8 dicembre 2011 [doc. *web* n. 1895743]

WP 189 - Documento di lavoro su epSOS
25 gennaio 2012 [doc. *web* n. 1895747]

Lettera del Gruppo Art. 29 alla Vicepresidente Reding relativa alla risposta del Gruppo Art. 29 alla Comunicazione della Commissione "Un approccio globale alla protezione dei dati personali nell'UE"

14 gennaio 2011 [doc. *web* n. 1895757]

Lettera del Gruppo Art. 29 sui nuovi negoziati UE riguardanti gli accordi PNR con gli Stati Uniti, Canada e Australia

19 gennaio 2011 [doc. *web* n. 1895761]

Lettera del Gruppo Art. 29 alla sig.ra F. Le Bail (direttore generale dell'Unità C3 presso la DG Giustizia) mirante a fornire contributi alla Commissione sulle prassi vigenti a livello nazionale, le problematiche nell'attuazione della Direttiva ed alcuni suggerimenti migliorativi o emendativi con riguardo alle categorie particolari di dati ("dati sensibili"), alla notifica dei trattamenti ed all'attuazione concreta dell'articolo 28, comma 6, della Direttiva 95/46/CE

All. A Documento consultivo sulle categorie particolari di dati ("dati sensibili")

All. B Documento consultivo sulla notifica dei trattamenti

All. C Documento consultivo sull'attuazione concreta dell'articolo 28, comma 6, della Direttiva 95/46/CE

20 aprile 2011 [doc. *web* nn. 1896292 e Allegati 1895773, 1895779, 1895787]

Lettera del Gruppo Art. 29 al Ministero del Tesoro degli Stati Uniti d'America (UST) in merito all'interpretazione dell'Accordo TFTP da parte dell'UST

7 giugno 2011 [doc. *web* n. 1895798]

Lettera del Gruppo art. 29 al Commissario Malmström in merito al Sistema di controllo delle transazioni finanziarie dei terroristi (TFTS) – Comunicazione della Commissione europea COM(2011) 429

29 settembre 2011 [doc. *web* n. 1895802]

Lettera del Gruppo Art.29 alla Commissione (DG Mercato Interno) sui trasferimenti internazionali di dati allo US Public Accounting Oversight Body-PCAOB

13 dicembre 2011 [doc. *web* n. 1895806]

Lettera del Gruppo Art. 29 al Commissario Barnier in merito alla proposta di Regolamento sulla cooperazione amministrativa attraverso il Sistema informativo del mercato interno (Regolamento IMI)

13 dicembre 2011 [doc. *web* n. 1895813]

23.3. 33MA CONFERENZA DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Risoluzione sull'accreditamento

1° novembre 2011 [doc. *web* n. 1895569]

Risoluzione sul protocollo Internet IPv6 (identificatori univoci)

1° novembre 2011 [doc. *web* n. 1895573]

Risoluzione sul coordinamento internazionale delle attività di implementazione delle norme in materia di *privacy*

1° novembre 2011 [doc. *web* n. 1895581]

Risoluzione sulla protezione dei dati e le catastrofi naturali

1° novembre 2011 [doc. *web* n. 1895585]

Risoluzione di Città del Messico

1° novembre 2011 [doc. *web* n. 1895589]

23.4. *SPRING CONFERENCE*

Risoluzione sull'esigenza di un quadro unitario di garanzie in materia di protezione dati

5 aprile 2011 [doc. *web* n. 1895593]

23.5. GRUPPO DI LAVORO IN MATERIA DI ATTIVITÀ GIUDIZIARIE E DI POLIZIA - *WPPJ*

Rapporto Annuale di attività per l'anno 2010

2011 [doc. *web* n. 1895957]

23.6. GRUPPO DI LAVORO INTERNAZIONALE SULLA PROTEZIONE DEI DATI NEL SETTORE DELLE TELECOMUNICAZIONI - *IWGDPT*

Documento di lavoro sui dispositivi di registrazione degli eventi (scatole nere)
4 aprile 2011 [doc. *web* n. 1895966]

Documento di lavoro sui micropagamenti effettuati via internet
13 settembre 2011 [doc. *web* n. 1895970]

Documento di lavoro su "contatori intelligenti", *"privacy by design"* e protezione dei dati
13 settembre 2011 [doc. *web* n. 1895974]

23.7. CONSIGLIO D'EUROPA

Documento sulla modernizzazione della Convenzione 108/1981
5 marzo 2012 [doc. *web* n. 1895978]

23.8. OCSE

Rapporto - Il mondo *privacy* in evoluzione: a 30 anni dalle linee-guida sulla *privacy* dell'OCSE
6 aprile 2011 [doc. *web* n. 1895983]

Rapporto - La protezione dei minori *online*
2 maggio 2011 [doc. *web* n. 1895991]

Rapporto Direttorato Health - Uso secondario dei dati sanitari a scopi di ricerca e di implementazione delle politiche sanitarie pubbliche
9 novembre 2011 [doc. *web* n. 1895987]