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

PAGINA BIANCA

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

1. Principali interventi dell'Autorità nel 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]);