posta di introdurre nell'ordinamento una disposizione che attribuisca espressamente al soggetto per conto del quale si effettua il contatto promozionale la titolarità del trattamento dei dati, in modo che, in caso di trattamento illecito, ne discenda la responsabilità solidale con la società che effettua le chiamate. Siffatta previsione dovrebbe indurre le società committenti a delegare l'attività promozionale a soggetti affidabili e in grado di rispettare la normativa in materia di protezione dei dati personali;

c) un'audizione tenutasi il 23 luglio 2014, presso la Commissione igiene e sanità del Senato nell'ambito dell'indagine conoscitiva sulle origini e gli sviluppi del cd. caso Stamina. Prendendo spunto dal dibattito seguito alla nota vicenda – che ha toccato picchi di "accanimento informativo" sino alla divulgazione dell'immagine "in chiaro" di una bimba malata –, il Garante ha formulato alcune considerazioni sull'incompatibilità di un certo modo di fare informazione con la disciplina posta a tutela della riservatezza, che si risolve nella violazione della dignità e del diritto del minore a non vedere esibita la propria identità e infermità (anche alla luce della Carta di Treviso e del codice deontologico dei giornalisti);

d) un'audizione informale, tenutasi il 29 maggio 2014 presso la Commissione affari costituzionali, della Presidenza del Consiglio e interni della Camera dei deputati in merito alla proposta di legge che modifica l'art. 24, l. 7 agosto 1990, n. 241, in materia di accesso dei membri del Parlamento ai documenti amministrativi per esigenze connesse allo svolgimento del mandato parlamentare (AC 1761).

### 3.3. *L'Autorità e le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento*

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 (cfr. sez. IV, tab. 11). In particolare, sono stati forniti elementi di valutazione ai fini della risposta, da parte del Governo, su:

a) un'interrogazione sugli *standard* di sicurezza nel trattamento dei dati da parte dei *social network* e in particolare di *Facebook* (n. 4-01112 dell'on. Bianconi: nota 18 dicembre 2014);

b) un'interrogazione sul cd. *datagate* (interrogazione a risposta scritta n. 4-04805 dell'on. Prodani: nota 30 ottobre 2014), tema sul quale l'Autorità già nel 2013 ha avuto modo di esprimersi in relazione a ben quattro atti di sindacato ispettivo presentati in Parlamento sull'argomento (cfr. Relazione 2013, p. 22);

c) un'interrogazione sulle modalità di rilascio del cud da parte dell'Inps (interrogazione a risposta in Commissione n. 5-02313, dell'on. Garavini: nota 4 agosto 2014);

d) tre mozioni concernenti l'impatto sulla protezione dei dati personali dell'accordo commerciale internazionale di partenariato transatlantico per il commercio e gli investimenti (TTIP) (mozione 1-00558 dell'on. Kronblicher: nota 8 agosto 2014; mozione n. 1-00490 dell'on. Gallinella: nota 24 giugno 2014; mozione 1-00413 dell'on. Migliore: nota 28 maggio 2014);

e) una mozione e un'interrogazione concernenti il trattamento dei dati personali nell'attività di promozione commerciale svolta mediante *call center*, con particolare riferimento ai casi in cui il servizio è delocalizzato in Paesi

terzi in applicazione delle disposizioni dell'articolo 24-*bis*, d.l. n. 83/2012, convertito dalla l. n. 134/2012) (mozione n. 1-00457, dell'on. Palazzotto: nota 2 luglio 2014); interrogazione a risposta in Commissione lavoro della Camera n. 5-01719, dell'on. Albanella: nota 31 gennaio 2014);

f) una mozione in materia di *cyberbullismo* (n. 1-00233 dell'on. Ferrara ed altri: nota 13 giugno 2014).

### 3.4. *L'attività consultiva del Garante sugli atti del Governo*

#### *3.4.1. I pareri sugli atti regolamentari e amministrativi del Governo*

Nel quadro dell'attività consultiva obbligatoria concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso il parere (obbligatorio) di competenza sugli schemi di numerosi provvedimenti (v. pure sez. IV, tab. 3), di seguito riportati:

1) decreto del Ministro dell'interno recante modifiche al regolamento 21 giugno 2006, n. 244, per l'aggiornamento e l'integrazione dei tipi di dati sensibili e giudiziari e delle relative operazioni di trattamento effettuate dal Ministero dell'interno, adottato ai sensi degli artt. 20, comma 2, e 21, comma 2, del Codice (parere 11 dicembre 2014, n. 582, doc. web n. 3708655);

2) decreto del Presidente della Corte dei conti recante le prime regole tecniche ed operative per l'utilizzo della posta elettronica certificata nei giudizi dinanzi alla Corte dei conti, adottato ai sensi dell'art. 20-*bis*, d.l. 18 ottobre 2012, n. 179, convertito dalla l. 17 dicembre 2012, n. 221 (parere 4 dicembre 2014, n. 556, doc. web n. 3624087);

3) provvedimento del Ministero del lavoro e delle politiche sociali recante il modello tipo della dichiarazione sostitutiva unica (Dsu), dell'attestazione riportante l'Isee e delle relative istruzioni per la compilazione (parere 6 novembre 2014, n. 495, doc. web n. 3515450);

4) convenzione-tipo tra l'ente gestore (Consap s.p.a.) e gli "aderenti diretti" al sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità (istituito dal d.lgs. 11 aprile 2011, n. 64), adottato ai sensi dell'art. 4, comma 3, del decreto del Ministro dell'economia e delle finanze 19 maggio 2014, n. 95, sul cui schema il Garante aveva reso a suo tempo parere (cfr. Relazione 2013, par. 3.2) (parere 9 ottobre 2014, n. 445, doc. web n. 3505427);

5) convenzione tra il Ministero dell'economia e delle finanze e taluni "aderenti indiretti" al medesimo sistema di prevenzione, sul piano amministrativo, delle frodi mediante furto d'identità, adottata ai sensi dell'art. 4, comma 2, del decreto del Ministro dell'economia e delle finanze 19 maggio 2014, n. 95 (parere 18 settembre 2014, n. 408, doc. web n. 3487835);

6) decreto del Ministro dell'economia e delle finanze concernente l'individuazione delle specifiche tecniche del sistema di conservazione informatica delle negoziazioni effettuate dagli esercenti l'attività di cambiavalute ai sensi dell'art. 17-*bis*, comma 4, d.lgs. 13 agosto 2010, n. 141 (parere 25 settembre 2014, n. 425, doc. web n. 3487879);

7) d.P.R. recante disposizione di attuazione della l. 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del dna e del laboratorio centrale per la banca dati nazionale del dna (parere 31 luglio 2014, n. 389, doc. web n. 3616088) (par. 9.2);

8) decreto interministeriale del Ministro dello sviluppo economico e del Ministro delle infrastrutture e dei trasporti recante il regolamento per l'istituzione e il funzionamento dell'"archivio informatico integrato" di cui all'art. 21, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221 (parere 24 luglio 2014, n. 378, doc. web n. 3320757);

9) d.P.C.M. recante il regolamento per l'attuazione dell'art. 21 (Esperti nazionali distaccati) della l. 24 dicembre 2012, n. 234, recante "Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea" (poi decreto 30 ottobre 2014, n. 184; parere 10 luglio 2014, n. 355, doc. web n. 3325197);

10) d.P.C.M. recante definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (Spid), nonché dei tempi e delle modalità di adozione del sistema Spid da parte delle pp.aa. e delle imprese (poi decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014; parere 19 giugno 2014, n. 311, doc. web n. 3265492);

11) decreto dirigenziale del Ministero della giustizia recante modifiche al decreto 5 dicembre 2012 concernente la consultazione diretta del sistema informativo del casellario giudiziale da parte delle pp.aa. e dei gestori di pubblici servizi, ai sensi dell'art. 39, d.P.R. n. 313/2002 (poi decreto 12 giugno 2014; parere 19 giugno 2014, n. 312, doc. web n. 3273289);

12) decreto interministeriale recante regole tecniche per la realizzazione e il funzionamento del sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp), nonché le regole per il connesso trattamento dei dati, ai sensi dell'art. 8, comma 4, d.lgs. 9 aprile 2008, n. 81 (parere 12 giugno 2014, n. 295, doc. web n. 3255963);

13) decreto interministeriale del Ministro dell'interno e del Ministro dell'economia e delle finanze recante disposizioni organizzative per la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza e istituzione dell'ufficio per la sicurezza (*security manager*) (parere 5 giugno 2014, n. 279, doc. web n. 3246681);

14) d.P.C.M. recante definizione dei criteri e delle modalità di destinazione della quota pari al due per mille dell'imposta sul reddito delle persone fisiche, in base alla scelta del contribuente, a favore di partiti politici, adottato ai sensi dell'art. 12, comma 3, d.l. 28 dicembre 2013, n. 149 (conv. dalla l. 21 febbraio 2014, n. 13, poi decreto 28 maggio 2014; parere 22 maggio 2014, n. 256, doc. web n. 3246663);

15) d.P.C.M. in materia di Fascicolo sanitario elettronico, adottato ai sensi dell'art. 12, comma 7, d.l. 18 ottobre 2012, n. 179 e dell'art. 13, comma 2-*quater*, d.l. 21 giugno 2013, n. 69 (parere 22 maggio 2014, n. 261, doc. web n. 3230826);

16) decreto del Ministro della giustizia concernente regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche nei casi previsti dal codice di procedura civile (art. 161-*ter* delle disposizioni per l'attuazione del codice di procedura civile) (parere 15 maggio 2014, n. 245, doc. web n. 3235478);

17) d.P.C.M. recante le modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) e definizione del piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente (parere 17 aprile 2014, n. 202, doc. web n. 3105794);

18) decreto del Ministro della giustizia recante modifiche al regolamento 22 dicembre 2006, n. 306, in materia di trattamento dei dati sensibili e giudiziari da parte del Ministero della giustizia (poi decreto 24 luglio 2014, n. 123, in *G.U.* 26 agosto 2014, n. 197; parere 10 aprile 2014, n. 201, doc. web n. 3104282);

19) decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità delle prove di ammissione al corso di laurea magistrale in medicina e chirurgia in lingua inglese per l'anno accademico 2014-2015 (poi decreto 21 febbraio 2014, in *G.U.* 12 marzo 2014, n. 59; parere 20 febbraio 2014, n. 82, doc. web n. 2972695);

20) decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità e i contenuti delle prove di ammissione ai corsi di laurea e di laurea magistrale ad accesso programmato per l'anno accademico 2014-2015 (poi decreto 5 febbraio 2014, in *G.U.* 7 marzo 2014, n. 55; parere 30 gennaio 2014, n. 38, doc. web n. 2924822);

21) decreto del Ministro del lavoro e delle politiche sociali concernente la costituzione presso l'Inps del Casellario dell'assistenza, adottato ai sensi dell'art. 13, comma, 4, d.l. 31 maggio 2010, n. 78, convertito, dalla l. 30 luglio 2010, n. 122 (parere 23 gennaio 2014, n. 26, doc. web n. 2922956);

22) regolamento recante "Disposizioni concernenti le modalità di funzionamento, accesso, consultazione e collegamento con il CED di cui all'art. 8 della legge 1 aprile 1981, n. 121, della Banca dati nazionale unica della documentazione antimafia, istituita ai sensi dell'art. 96 del decreto legislativo 6 settembre 2011, n. 159" (parere 30 gennaio 2014, n. 39, doc. web n. 2924878).

Diversamente da quanto accaduto negli anni precedenti, nel 2014 non si sono registrati casi di mancata consultazione del Garante in relazione a provvedimenti aventi un particolare impatto sulla protezione dei dati personali (ai sensi del medesimo art. 154, comma 4, del Codice). Ciò è, evidentemente, il segno di una accresciuta sensibilità delle pubbliche amministrazioni sulla protezione dei dati personali – frutto anche dell'approccio collaborativo dell'Autorità (sin dalla fase di elaborazione dei testi da sottoporre a parere) – e in particolare sull'utilità per le amministrazioni stesse del coinvolgimento dell'Autorità nella valutazione dei riflessi dei provvedimenti normativi sui diritti alla riservatezza e alla protezione dei dati delle persone.

*3.4.2. I pareri su norme di rango primario*

Su specifica richiesta del Governo il Garante ha inoltre reso parere su alcuni atti normativi del Governo aventi rango primario. L'art. 154, comma 4, del Codice, infatti, fa riferimento alla normativa avente rango secondario, anche se la correlata disposizione della direttiva europea non reca una distinzione al riguardo (art. 28, paragrafo 2). Le richieste di parere su atti primari si inquadrano in un contesto collaborativo che l'Autorità, come più volte segnalato alla Presidenza del Consiglio, auspica possa ulteriormente svilupparsi, nella consapevolezza che sia di grande utilità il coinvolgimento del Garante nella fase preparatoria di iniziative legislative, oltre che regolamentari, del Governo al fine di valutarne previamente l'impatto sulla protezione dei dati personali e sui diritti delle persone. I pareri hanno riguardato in particolare:

a) Scambio transfrontaliero di dati su infrazioni stradali

Uno schema di decreto legislativo di recepimento della direttiva 2011/82/UE in materia di scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, adottato in attuazione della l. 6 agosto 2013, n. 96 e volto a consentire lo scambio fra Paesi appartenenti all'Unione europea delle informazioni relative ai veicoli (e al rispettivo proprietario o intestatario) con i quali è stata commessa un'infrazione stradale, fra quelle individuate nella direttiva, in uno Stato membro diverso da quello di immatricolazione (poi d.lgs. 4 marzo 2014, n. 37; parere 9 gen-

naio 2014, n. 2, doc. web n. 2904320). Lo schema di decreto è stato predisposto all'esito dei lavori di un tavolo tecnico istituito presso la Presidenza del Consiglio dei ministri-Settore legislativo del Ministro per gli affari europei, cui ha fornito, a richiesta, il proprio contributo anche l'Ufficio, per quanto riguarda gli aspetti di protezione dei dati personali. Lo schema poi sottoposto a parere dell'Autorità non presentava criticità. Di particolare importanza è l'art. 10 dello schema che attribuisce all'interessato (che può essere anche il cittadino di un altro Stato UE, che ha commesso un'infrazione in Italia) due "nuovi" diritti (non previsti, allo stato, dalla normativa vigente e in particolare dal Codice), e cioè il diritto di ottenere: 1) che i dati non vengano cancellati, ma solo conservati temporaneamente se vi sono fondati motivi di ritenere che la cancellazione possa compromettere un proprio legittimo interesse, e trattati ulteriormente solo per lo scopo che ne ha impedito la cancellazione; 2) che sia data evidenza (mediante un indicatore di validità) ai dati di cui l'interessato contesta l'esattezza (cd. diritto di *flag*). Tali diritti sono esercitati con le modalità previste dal Codice e tutelati ricorrendo al Garante o all'autorità giudiziaria. Oltre a tali diritti, l'art. 10 del decreto "conferma" gli altri diritti dell'interessato già previsti dal Codice (ad esempio: rettifica, cancellazione, informativa) nei limiti ivi stabiliti (ad es., l'informativa non è dovuta rispetto a trattamenti effettuati per finalità di prevenzione, accertamento o repressione di reati quali sono alcune fattispecie di infrazioni stradali oggetto della direttiva e del decreto: guida in stato di ebbrezza o sotto l'influsso di stupefacenti *ex* artt. 186, 186-*bis* e 187 del codice della strada). Queste disposizioni sono state introdotte in attuazione della decisione quadro 2008/977/GAI, del Consiglio del 27 novembre 2008, concernente la protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale, richiamata espressamente nella direttiva quale parametro di conformità. Tale decisione, com'è noto, non risulta ancora attuata in Italia malgrado le ripetute sollecitazioni dell'Autorità; tuttavia il richiamo contenuto nella direttiva europea ne ha reso necessaria l'implementazione limitatamente allo scambio di informazioni sulle infrazioni stradali, al fine di evitare l'instaurazione di procedure d'infrazione per mancato recepimento della direttiva stessa. Nel parere, pertanto, l'Autorità ha segnalato alla Presidenza del Consiglio la complessità ed i rischi di una "attuazione parziale" della decisione quadro, per la difficoltà di adattare le disposizioni in materia di protezione dei dati personali in essa contenute – concepite, ovviamente, in relazione agli scambi informativi per ogni tipologia di cooperazione giudiziaria e di polizia – a scambi di dati in specifici settori.

b) Ordine di protezione europeo

Uno schema di decreto legislativo per il recepimento della direttiva europea 2011/99/UE in materia di "ordine di protezione europeo", la quale prevede un meccanismo di mutuo riconoscimento dell'efficacia di provvedimenti adottati in materia penale dalle competenti autorità giurisdizionali nazionali (misure di protezione), finalizzati alla protezione di vittime di reati rispetto al pericolo di condotte idonee a ledere i loro diritti fondamentali (vita, integrità fisica, psichica o sessuale, dignità e libertà personale), come ad esempio rapimenti, molestie, *stalking*. Lo schema di decreto legislativo regolamenta, sul piano processuale, i presupposti per il riconoscimento all'estero degli effetti di una misura di protezione adottata dalle autorità italiane nonché quelli necessari per il riconoscimento in Italia degli effetti di un provvedimento emesso da autorità di altri Stati membri. Anche in questo caso, l'Ufficio ha partecipato ad un tavolo di lavoro presso la Presidenza del Consiglio dei ministri fornendo il proprio contributo in vista del successivo parere dell'Autorità (parere 30 ottobre 2014, n. 481, doc. web n. 3657992). Anche in tale materia il Governo ha

ritenuto indispensabile provvedere ad un'attuazione "parziale" della medesima decisione quadro 2008/977/GAI, richiamata nel considerando 36 della direttiva, per non incorrere in una procedura d'infrazione, introducendo, in relazione agli scambi informativi in materia di ordine di protezione europeo, disposizioni analoghe a quelle contenute nel d.lgs. n. 37/2014 sulle infrazioni stradali, sopra descritte (v. punto a). Lo schema, infatti, all'art. 15, dopo avere previsto l'applicazione ai trattamenti di dati effettuati ai sensi del decreto delle disposizioni contenute nella Parte II, Titolo I del Codice (Trattamenti in ambito giudiziario), attribuisce all'interessato, con le opportune precisazioni rese necessarie dalla specificità della materia, i due "nuovi" diritti alla conservazione temporanea dei dati in luogo della cancellazione e alla "evidenza" dell'esercizio dei diritti stessi. Ovviamente, l'Autorità in occasione del parere ha rinnovato la forte preoccupazione per i rischi derivanti da una "attuazione parziale" della Decisione-quadro.

c) Appartenenza a gruppo linguistico

Uno schema di decreto legislativo in materia di dichiarazione di appartenenza o aggregazione al gruppo linguistico nella Provincia di Bolzano, volto a integrare l'art. 20-*ter*, d.P.R. 26 luglio 1976, n. 752 (recante norme di attuazione dello Statuto speciale della Regione Trentino-Alto Adige in materia di proporzionale negli uffici statali della provincia e di conoscenza delle due lingue nel pubblico impiego), introdotto dal d.lgs. 23 maggio 2005, n. 99. L'art. 20-*ter* prevede che, al fine di poter beneficiare, nei casi previsti, degli effetti giuridici derivanti dall'appartenenza o dall'aggregazione al gruppo linguistico, ogni cittadino maggiorenne non interdetto, residente nella provincia, ha facoltà di rendere in ogni momento una dichiarazione individuale nominativa di appartenenza ad uno dei tre gruppi linguistici italiano, tedesco e ladino (art. 20-*ter*, comma 1, d.P.R. n. 752/1976). Lo schema di decreto era volto ad estendere il vigente regime normativo ai cittadini non residenti nella Provincia di Bolzano, anche se appartenenti ad altro stato dell'Unione europea, nonché ai cittadini di Paesi terzi titolari del permesso di soggiorno CE per soggiornanti di lungo periodo. La Presidenza del Consiglio dei ministri aveva già inoltrato a suo tempo richiesta di parere su una analoga proposta integrativa dell'art. 20-*ter*, che si riferiva però ai soli cittadini di altro stato dell'Unione europea. Nell'esprimere parere favorevole su tale precedente schema di decreto (parere 10 gennaio 2008) il Garante si era limitato a prendere atto della scelta allora operata dall'Amministrazione di non prendere in considerazione nella predetta estensione i cittadini appartenenti a Paesi terzi. L'Autorità, pertanto, non riscontrando nel testo ulteriori aspetti di criticità sotto il profilo della protezione dei dati personali, ha confermato l'avviso favorevole già espresso a suo tempo (parere 10 luglio 2014, n. 354, doc. web n. 3320726).

### 3.5. *L'esame delle leggi regionali*

È proseguita l'attività di esame del Garante 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 circa la compatibilità delle stesse con le disposizioni in materia di protezione dei dati personali e con il dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.). L'Autorità, nel corso dell'anno, ha esaminato 16 leggi regionali e, in linea generale, ha riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale in relazione agli aspetti di protezione dei dati personali.

Solo in un caso sono stati forniti alla Presidenza del Consiglio elementi da valutare ai fini di una eventuale illegittimità costituzionale delle disposizioni normative e precisamente in relazione alla legge della Regione Calabria 18 dicembre 2013, n. 53, recante Disciplina del sistema regionale dell'istruzione e formazione professionale (nota 4 febbraio 2014).

Le osservazioni hanno riguardato l'art. 14 della legge che istituisce l'"anagrafe regionale degli studenti" (Ans), alimentata dalle informazioni sui percorsi degli studenti a partire dal primo anno della scuola primaria e "coordinata ed integrata" con l'anagrafe nazionale (comma 3). La disposizione disciplina altresì i flussi di dati che la Giunta può comunicare all'ufficio scolastico regionale, a quelli provinciali nonché ai comuni e ad altre istituzioni formative (agenzie formative accreditate e istituti professionali) (commi 6 e 7).

Premesso che il legislatore, disciplinando congiuntamente profili inerenti l'istruzione e la protezione dei dati personali, nell'ambito delle proprie competenze legislative esclusive, ha posto specifici vincoli alla residuale competenza legislativa regionale in materia (artt. 33, 117, secondo comma, lett. *l*), *m*), *n*), *r*), e terzo comma, Cost.), il Garante ha rilevato che le regioni possono costituire le proprie anagrafi regionali degli studenti nei limiti di quanto previsto dalla normativa nazionale (d.lgs. n. 76/2005) evitando la duplicazione di banche dati che possano contenere informazioni similari (d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221) e prevedendo la funzione di coordinamento del Ministero dell'istruzione, dell'università e della ricerca, da esercitarsi sentito il Garante (art. 13, d.l. 12 settembre 2013, n. 104, convertito dalla l. 8 novembre 2013, n. 128). In ogni caso le regioni possono effettuare il trattamento di dati personali nel rispetto dei presupposti e dei limiti stabiliti dal Codice (Corte cost. n. 271/2005), disciplina dettata dal legislatore nell'ambito della propria competenza esclusiva di cui all'art. 117, secondo comma, lett. *l*) ed *r*), Cost. Al riguardo, deve evidenziarsi, in particolare, che i soggetti pubblici possono trattare dati personali necessari, pertinenti e non eccedenti rispetto alle proprie specifiche funzioni istituzionali (artt. 3, 11, 18 del Codice).

Sulla base del predetto quadro normativo, si è ritenuto necessario segnalare alla Presidenza, per le conseguenti determinazioni, le seguenti criticità: 1) per quanto riguarda l'integrazione dell'anagrafe regionale con l'Ans (art. 14, comma 3), l'esigenza di assicurare il rispetto della funzione di coordinamento del Miur nell'integrazione e coordinamento delle banche dati del sistema nazionale delle anagrafi (art. 13, comma 2, d.l. n. 104/2013); 2) con riferimento ai dati contenuti nell'anagrafe regionale e ai flussi informativi (art. 14, commi 4, 6 e 7), il divieto di duplicazione di banche dati (in quanto alcune delle informazioni raccolte nella costituenda anagrafe regionale degli studenti sembravano essere già presenti nell'Ans, specie quelle relative al percorso scolastico: art. 10, comma 8, d.l. n. 179/2012) nonché il rispetto dei principi di pertinenza e non eccedenza delle informazioni raccolte nella predetta anagrafe e comunicate ad altri soggetti, anche mediante non meglio definiti "collegamenti" con i dati raccolti da altri settori (comma 4).

La legge regionale non è stata impugnata. Nondimeno la Regione Calabria ha valutato di integrare il comma 3 dell'art. 14 con il riferimento alla normativa nazionale segnalata dal Garante al fine di assicurare il rispetto delle funzioni di coordinamento del Ministero in tale materia, anche sotto il profilo della protezione dei dati personali (art. 1, l.r. 20 febbraio 2014, n. 5, in *Bur* 21 febbraio 2014, n. 8).

# II - L'attività svolta dal Garante

## 4 Il Garante e le pubbliche amministrazioni

### 4.1. *I regolamenti sui trattamenti di dati sensibili e giudiziari*

**ADAMS**

Dopo aver espresso parere favorevole rispetto al regolamento per il trattamento di dati sensibili e giudiziari adottato dal Comitato olimpico nazionale italiano (Coni) nel 2007 (provv. 19 settembre 2007, doc. web n. 1443411), il Garante è tornato ad esprimersi sul nuovo schema contenente talune modifiche e integrazioni motivate dalla necessità per il Coni di perseguire l'interesse pubblico sotteso alle attività di prevenzione e repressione del fenomeno del *doping* nello sport attraverso l'uso dell'*Anti-Doping Administration & Management System* (sistema ADAMS) (provv. 31 luglio 2014, n. 390, doc. web n. 3385186). Ciò nelle more della definizione, a livello europeo, di un quadro di garanzie unitario volto ad assicurare la conformità alla disciplina di protezione dei dati di alcuni aspetti della regolamentazione *anti-doping* fissata nel codice mondiale in materia e negli *standard* che lo completano (v. provv. 13 ottobre 2008, doc. web n. 1563970; pareri del Gruppo Art. 29 n. 3/2008 - WP 156, doc. web n. 1619614 e n. 4/2009 - WP 162, doc. web n. 1620339; lettere del Gruppo Art. 29 a WADA, doc. web nn. 2983092 e 2983102).

Come è noto, il sistema ADAMS, realizzato dall'Agenzia mondiale *anti-doping* (*World Anti-Doping Agency*-WADA), è costituito da una banca dati riferita agli atleti per pianificare e coordinare i controlli *anti-doping* situata in Canada (Québec). In particolare, sulla base delle regole fissate nel codice mondiale e nei relativi *standard*, sono registrati nella banca dati a cura degli stessi atleti, delle organizzazioni nazionali *anti-doping* e delle federazioni sportive di appartenenza dati identificativi e altre informazioni riferite all'atleta, quali i dati sui luoghi di reperibilità e permanenza (cd. *whereabouts*), sulle esenzioni a fini terapeutici, sulla pianificazione e distribuzione dei controlli *anti-doping* e sui singoli controlli effettuati.

Il parere è stato reso su una versione aggiornata dello schema tipo di regolamento all'esito di un proficuo lavoro di collaborazione con i competenti uffici del Coni, i quali, a seguito di numerose riunioni e contatti informali, hanno accolto le osservazioni formulate dall'Ufficio. Gli elementi forniti all'Autorità sono stati ritenuti idonei a garantire un adeguato quadro giuridico per i trattamenti di dati sensibili e giudiziari, effettuati dal Coni attraverso la banca dati ADAMS in quanto ente istituzionalmente preposto all'adozione e all'attuazione della normativa *anti-doping* (d.lgs. 23 luglio 1999, n. 242; Statuto del Coni; norme sportive *anti-doping*; artt. 18 ss. del Codice).

Tali trattamenti, che comportano flussi transfrontalieri di dati personali anche verso Paesi terzi (cfr. in merito anche par. 23.3) – limitati ai soli dati indispensabili ed effettuati mediante operazioni di trattamento non massive o ripetute –, risultano infatti necessari per il contrasto al *doping* e sono quindi riconducibili alle finalità di rilevante interesse pubblico individuate dal Codice, di applicazione della normativa in materia di sicurezza e salute della popolazione e di promozione dello sport (l. 14

dicembre 2000, n. 376; artt. 43, comma 1, lett. *c*), 73, comma 2, lett. *c*), e 85, comma 1, lett. *e*), del Codice). In particolare, i trattamenti di dati personali così effettuati dal Coni riguardano soltanto un gruppo selezionato di atleti (quelli inseriti nel *registered testing pool* nazionale), ferma restando la facoltà del Coni di disporre controlli anche su altri atleti. Con riferimento ai predetti atleti, il Coni potrà pertanto effettuare, ove necessario, operazioni di trasferimento all'estero di dati personali, anche sensibili e giudiziari, verso la banca dati ADAMS e verso le organizzazioni *anti-doping* ubicate anche in Paesi terzi di volta in volta competenti a testare gli atleti sulla base delle regole *dell'anti-doping*.

Altre indicazioni fornite dall'Ufficio, recepite dal Coni nel nuovo schema di regolamento, hanno riguardato le cautele previste a tutela dei diritti degli interessati nella pubblicazione sul sito istituzionale del Coni dei dati giudiziari contenuti nelle sentenze e negli altri provvedimenti adottati dagli organi di giustizia sportiva effettuati per finalità di comunicazione istituzionale e di informatica giuridica.

**Regolamenti di dati sensibili e giudiziari**

Sul tema dei regolamenti sul trattamento dei dati sensibili e giudiziari da parte di amministrazioni locali, l'Autorità è stata consultata dal Comune di Palermo prima dell'approvazione di un nuovo regolamento in sostituzione di quello previgente. In particolare, è stato richiesto se il nuovo regolamento potesse discostarsi dallo schema approvato con parere del Garante del 21 settembre 2005 e prevedere che l'identificazione e la pubblicazione dei tipi di dati e delle operazioni eseguibili potessero essere rinviate dal regolamento stesso ad un atto rimesso ai singoli settori, in ragione della competenza specialistica di ciascuno di essi. Al riguardo, l'Ufficio ha precisato che le amministrazioni non possono avvalersi di meri atti, i quali, anche quando (formalmente) denominati regolamenti, non hanno la necessaria natura di fonte normativa suscettibile di incidere su diritti e libertà fondamentali di terzi, dovendo assicurare l'emanazione dell'atto di natura regolamentare previsto dalla norma, anche promuovendone l'adozione da parte dell'organo competente in base all'ordinamento dell'amministrazione. La soluzione prospettata dal Comune, che intenderebbe rimettere ai singoli dirigenti dei settori l'adozione degli atti necessari a identificare e rendere pubblici i dati sensibili e le operazioni eseguibili, non è stata pertanto ritenuta conforme alle previsioni del Codice, con conseguente illeceità dei trattamenti di dati personali eventualmente effettuati su tali presupposti (note 11 aprile e 23 maggio 2014).

**Unar**

Con parere favorevole del 5 giugno 2014, n. 280 (doc. web n. 3248445), il Garante si è espresso sulle modifiche ed integrazioni apportate alla scheda n. 6 del regolamento per il trattamento di dati sensibili e giudiziari della Presidenza del Consiglio dei ministri relativa alla "Gestione degli interventi in ambito sociale, di pari opportunità e tutela dei soggetti vittime della discriminazione", effettuati dall'Ufficio nazionale antidiscriminazioni razziali (Unar) (d.P.C.M. 30 novembre 2006, n. 312).

La predetta scheda è stata modificata con l'aggiunta, nell'ambito della sezione relativa ai tipi di dati trattati, de "lo stato di salute: patologie attuali, patologie pregresse, terapie in corso anamnesi familiare"; e de "la vita sessuale". L'Unar ha rappresentato, sulla base del quadro normativo di seguito riportato, l'indispensabilità del trattamento dei predetti dati personali di natura sensibile in ragione del recente ampliamento dei compiti attribuiti all'Ufficio stesso (art. 22, comma 3, del Codice). In particolare, in base al d.P.C.M. 1° ottobre 2012, "il Dipartimento per le pari opportunità è la struttura di supporto al Presidente che opera nell'area funzionale inerente alla promozione ed al coordinamento delle politiche dei diritti della persona, delle pari opportunità e della parità di trattamento e delle azioni di Governo volte a prevenire e rimuovere ogni forma e causa di discriminazione" e "nell'ambito del

Dipartimento opera altresì l'Ufficio per la promozione delle parità di trattamento e la rimozione delle discriminazioni fondate sulla razza e sull'origine etnica di cui all'art. 29 della legge 1° marzo 2002, n. 39" (art. 16, commi 1 e 5).

Anche il successivo d.m. 4 dicembre 2012 ha ampliato i compiti affidati all'Unar, attribuendogli la funzione di garantire l'effettività del principio di parità di trattamento tra le persone e di vigilare sull'operatività degli strumenti di tutela vigenti contro le discriminazioni fondate su tutti i fattori di comportamenti discriminatori con particolare riferimento a quelle derivanti dalla razza e dall'origine etnica (art. 8, comma 1). A tal fine, il Servizio per la tutela della parità di trattamento presso l'Unar si occupa, in particolare, di gestire la raccolta delle segnalazioni in ordine a casi di discriminazione.

### 4.2. *Le grandi banche dati pubbliche*

**Inps**

Lo schema di convenzione redatto dall'Inps ai sensi dell'art. 58, comma 2, del Cad, per la fruibilità telematica delle proprie banche dati ha formato oggetto di esame da parte del Garante. La richiamata disposizione prevede che le amministrazioni titolari di banche dati accessibili per via telematica predispongano apposite convenzioni, aperte all'adesione di tutte le amministrazioni interessate, volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Sul tema, l'Autorità è già intervenuta nel 2013 con un parere favorevole reso all'Agenzia per l'Italia Digitale (AgID) riguardante le "Linee guida per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni" (v. provv. 4 luglio 2013, n. 332, doc. web n. 2574977; v. anche Relazione 2013, p. 36). Il richiamato quadro normativo di settore disciplinato dall'art. 58, c. 2, del Cad, è stato modificato dalla legge 11 agosto 2014, n. 114: con l'innovazione introdotta si prevede che le pubbliche amministrazioni comunichino tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'art. 72, comma 1, lett. *e*). L'AgID, sentiti il Garante e le amministrazioni interessate alla comunicazione telematica, è chiamata a definire gli *standard* di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi.

In ragione della rilevanza dei dati, anche sensibili, trattati presso i sistemi informativi dell'Inps e dell'ingente numero di soggetti legittimati ad accedervi, si è esaminato lo schema di convenzione quadro predisposto dell'Inps sulla base delle predette "Linee guida" al fine di verificare la necessità di individuare ulteriori misure e accorgimenti. Lo schema, elaborato dall'Istituto alla luce degli approfondimenti svolti in collaborazione con l'Ufficio, anche nel corso di accertamenti ispettivi, riguarda soltanto gli accessi delle pp.aa. e dei gestori di pubblico servizio per finalità di controllo delle autocertificazioni e per finalità istituzionali e non fa riferimento agli accessi da parte di intermediari, caf e patronati. Il documento ha ottenuto il parere favorevole del Garante in considerazione delle specifiche misure e degli accorgimenti, anche di carattere organizzativo, ivi previsti, ritenuti idonei a ridurre al minimo i rischi per la sicurezza dei dati, tenuto conto delle particolari caratteristiche dei trattamenti effettuati presso l'Istituto (provv. 6 marzo 2014, n. 108, doc. web n. 3033479).

A seguito dei numerosi casi di accessi abusivi ai sistemi informativi dell'Inps (v. già Relazione 2013, p. 38), in relazione ai quali sono in corso ulteriori verifiche da parte dell'Istituto, l'Ufficio ha segnalato l'esigenza di approntare opportune misure tecniche e organizzative per bloccare tempestivamente eventuali accessi impropri e per prevenire il rischio che tali illeciti si ripetano (note 27 maggio e 28 agosto 2014).

Al riguardo, merita segnalare che, nell'ambito degli approfondimenti ispettivi riguardanti l'accesso dall'esterno alle banche dati dell'Inps, l'Istituto ha comunicato all'Autorità di aver intrapreso un processo di ridefinizione delle misure di sicurezza riguardanti l'accesso ai propri sistemi informativi da parte di soggetti esterni abilitati (professionisti, caf e patronati). Sulla base delle risultanze emerse nel corso di tali approfondimenti e delle interlocuzioni intercorse con l'Ufficio, le misure predisposte prevedono, in particolare, la digitalizzazione e la trasmissione telematica da parte degli intermediari di copia del documento di riconoscimento dell'interessato e del mandato da questi conferito all'intermediario al fine di prevenire i rischi di accessi indebiti volti al rilascio delle certificazioni unificate dei redditi di lavoro dipendente, equiparati e assimilati (cud). L'Inps ha altresì comunicato di aver avviato la messa a punto di un nuovo sistema di controllo e di *audit* finalizzato a verificare la regolarità degli accessi alle proprie banche dati da parte di intermediari esterni; in particolare, l'Istituto intende introdurre un sistema di blocco automatico preventivo degli accessi anomali (per contrastare il *download* massivo di dati contributivi tramite procedure robotizzate e i casi di ripetute visualizzazioni di cud da parte di diversi operatori), nonché implementare un sistema di monitoraggio a posteriori degli accessi al fine di verificare la sussistenza presso l'intermediario del documento di riconoscimento dell'interessato e del mandato dallo stesso conferito. Tali misure, in corso di definizione in seno all'Inps, saranno portate a conoscenza dell'Autorità per le valutazioni di competenza.

**Spid**

Come riferito (par. 3.4.1), il Garante ha reso parere su uno schema di decreto del Presidente del Consiglio dei ministri recante la definizione delle caratteristiche del "Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (Spid) nonché dei tempi e delle modalità di adozione del sistema da parte delle pubbliche amministrazioni e delle imprese, adottato ai sensi dell'articolo 64 del Cad (parere 19 giugno 2014, n. 311, doc. web n. 3265492). Il decreto esaminato è un primo provvedimento adottato in materia, le cui disposizioni, anche per i profili di protezione dei dati, rinviano a successivi atti che dovranno essere adottati dall'Agenzia per l'Italia digitale (AgID), previo parere dell'Autorità, e in cui saranno specificate le regole tecniche e le modalità attuative per la realizzazione dello Spid, le modalità di accreditamento dei soggetti coinvolti, le procedure per il rilascio dell'identità digitale, nonché le convenzioni sulla verifica e l'uso dei dati.

L'identità digitale è l'insieme degli attributi identificativi della persona, fisica o giuridica, raccolti e registrati in forma digitale. In sostanza si tratta di un codice identificativo univoco dotato di attributi identificativi obbligatori (codice fiscale, nome, cognome, comune di nascita, sesso) nonché di attributi secondari, quali la casella Pec, il numero di telefono fisso o mobile e di attributi qualificati (ad es. la qualifica professionale). Infine a ogni identità è associata una credenziale per accedere, tramite autenticazione informatica, ai servizi erogati in rete.

L'identità digitale è rilasciata dai "gestori dell'identità digitale", persone giuridiche che devono accreditarsi presso l'AgID e sono iscritti nel registro pubblico Spid. I gestori conservano, rendono disponibili e gestiscono gli attributi e le credenziali di autenticazione utilizzati dall'utente per l'accesso ai servizi. Il rilascio dell'identità digitale presuppone la verifica dell'identità del richiedente che può avvenire attraverso un contatto diretto (unico livello di verifica mantenuto per garantire un alto livello di sicurezza, anche se non in linea con altri progetti europei). Tale verifica può essere effettuata in diversi modi. Il riconoscimento *de visu* non è però sempre richiesto: se il richiedente possiede già un documento digitale di identità (CIE, CNS, TS-CNS) l'identità Spid potrà essere rilasciata senza ripetere la verifica, con una semplice richiesta *online*.

Oltre ai gestori di identità, sono coinvolti nel Sistema i "gestori di attributi qualificati" – ovvero soggetti che per legge sono titolati a certificare alcuni attributi qualificanti, come ad esempio un'abilitazione professionale, anch'essi accreditati presso l'AgID – e i "fornitori dei servizi", soggetti pubblici o privati che sottoscrivono apposite convenzioni con AgID e che erogano servizi via internet per i quali sia richiesta l'identificazione e l'autenticazione degli utenti. Tutti questi soggetti sono iscritti nel registro Spid.

Nel suo complesso, il Sistema è volto a favorire la diffusione di servizi in rete e ad agevolare l'accesso agli stessi mediante l'attribuzione a ciascun soggetto interessato di un'"identità digitale" allo scopo di identificare in modo univoco chi si rivolge, ad esempio, alla pubblica amministrazione per richiedere il servizio (come il rilascio di un certificato). L'istituzione di un sistema pubblico di identità dovrebbe consentire di disporre di identità digitali "sicure", in grado cioè di minimizzare anche i rischi di crimini informatici come il furto d'identità.

Il Garante ha espresso parere favorevole sullo schema di decreto, subordinandolo però al recepimento di numerose condizioni volte a perfezionare il testo e a renderlo conforme alla disciplina in materia di protezione dei dati personali.

L'architettura del sistema – anche se soggetto a conferma nei documenti attuativi – dovrebbe consentire ai cittadini di rivolgersi a vari gestori di identità e di dotarsi di più strumenti di identificazione, da utilizzare a seconda dei diversi contesti, anche tenendo conto del livello di sicurezza di volta in volta richiesto.

Il Sistema dovrebbe lasciare in vita la possibilità di utilizzare, per l'accesso ai servizi, anche la carta d'identità elettronica e la carta nazionale dei servizi. Tuttavia, mentre queste ultime presuppongono che i dati necessari per verificare l'identità in rete siano tutti disponibili al soggetto che offre il servizio, con Spid dovrebbero essere forniti a quest'ultimo solo i dati strettamente necessari per lo specifico servizio reso: ad esempio, se è necessario sapere unicamente che il richiedente è maggiorenne, potrà essere fornita solo tale informazione e non anche l'indirizzo di residenza o la data di nascita.

Inoltre, la presenza di più gestori di identità evita i rischi connessi alla creazione di una banca dati centralizzata delle identità, scongiurando che il sempre possibile suo malfunzionamento o violazione della stessa porti al crollo dell'intero sistema o a danni gravissimi per gli interessati.

Naturalmente, tutti questi aspetti, che astrattamente dovrebbero essere positivi dal punto di vista della protezione dei dati personali, dovranno essere verificati, attraverso l'esame degli atti applicativi, in sede di parere del Garante, oltre che nel funzionamento in concreto del Sistema.

**Casellario dell'assistenza**

Come anticipato (par. 3.4.1), l'Autorità si è altresì occupata dell'anagrafe generale delle posizioni assistenziali costituita presso l'Inps come partizione del Sistema informativo dei servizi sociali di cui all'art. 21, l. 8 novembre 2000, n. 328 (di seguito Siss) che raccoglie informazioni sulle prestazioni sociali erogate, sulle caratteristiche personali e familiari nonché sulla valutazione del bisogno dei beneficiari di tali prestazioni (cd. Casellario dell'assistenza: provv. 23 gennaio 2014, n. 26, doc. web n. 2922956). Si è così inteso assicurare una compiuta conoscenza dei bisogni sociali e consentire il monitoraggio della spesa e la programmazione, la valutazione dell'efficienza e dell'efficacia degli interventi nonché l'elaborazione di statistiche e la conduzione di studi e di ricerche nel settore dell'assistenza sociale. A questo scopo, le amministrazioni locali e ogni altro ente che eroga tali prestazioni devono mettere a disposizione del Casellario le informazioni previste dal decreto – quali i dati riguardanti le caratteristiche socio-demografiche e familiari dei beneficiari, nonché le informazioni sugli enti eroganti e sulle prestazioni erogate – e l'Inps deve renderle

disponibili in forma individuale, ma prive di ogni riferimento che ne permetta il collegamento con gli interessati o li renda comunque identificabili, al Ministero del lavoro, al Ministero dell'economia e delle finanze, alle Regioni, alle Province autonome e ai Comuni.

Inoltre, nel caso in cui all'erogazione della prestazione sia associata la presa in carico da parte del servizio sociale, è previsto che in apposite sezioni separate, dedicate alle persone non autosufficienti, in condizioni di povertà e ai minori in condizioni di disagio siano raccolte anche informazioni sulla valutazione del bisogno sociale. I dati direttamente identificativi dei beneficiari sono consultabili dagli enti locali con riferimento alle prestazioni da essi erogate e a quelle erogate dall'Inps. Garanzie ulteriori, volte a prevenire l'identificabilità degli interessati, sono previste per le informazioni contenute nella sezione dedicata ai minori in condizioni disagio. Hanno infine accesso alla banca dati la Guardia di finanza e l'Agenzia delle entrate per effettuare controlli sui beneficiari delle prestazioni.

Nello schema di decreto sottoposto all'Autorità, che ha recepito le indicazioni suggerite dall'Ufficio al Ministero del lavoro nel corso di riunioni e contatti informali, sono state circoscritte le tipologie di prestazioni sociali destinate a confluire nel Casellario prevedendo, in particolare, che questo raccolga informazioni connesse alle sole prestazioni sociali per la cui erogazione è necessaria l'identificazione del beneficiario. In considerazione dell'estrema delicatezza dei dati trattati e della vulnerabilità degli interessati, sono state inoltre definite le modalità di aggregazione e di anonimizzazione delle informazioni relative ai minori in situazione di disagio. Infine, l'Ufficio è intervenuto nella delimitazione dei soggetti legittimati ad accedere al Casellario e nella specificazione dei presupposti, finalità e modalità di accesso. Le modalità attuative e le specifiche tecniche per la raccolta, la trasmissione, lo scambio e l'anonimizzazione dei dati, nonché le misure di sicurezza del Casellario saranno definite dall'Inps con successivi decreti, sentito il parere del Garante.

**Dsu**

Parere favorevole è stato espresso sullo schema di provvedimento del Ministero del lavoro e delle politiche sociali di approvazione del modello tipo di dichiarazione sostitutiva unica (Dsu) per il calcolo dell'Indicatore della situazione economica equivalente (Isee), ai sensi dell'art. 10, comma 3, d.P.C.M. 5 dicembre 2013, n. 159 (provv. 6 novembre 2014, n. 495, doc. web 3515450). Come è noto, il citato d.P.C.M. n. 159/2013 – recante il regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'Isee, sul cui schema il Garante aveva fornito il parere di competenza (22 novembre 2012, n. 361, doc. web n. 2174496) – prevede che l'Isee venga calcolato sulla base delle informazioni, relative al nucleo familiare di appartenenza del beneficiario, fornite dal dichiarante attraverso un apposito modello di dichiarazione ("dichiarazione sostitutiva unica" – Dsu) nonché delle altre informazioni disponibili negli archivi dell'Inps e dell'Agenzia delle entrate, acquisite dal sistema informativo dell'Isee (artt. 2, comma 6, e 11).

Ciò premesso, il parere in esame è stato reso su una versione di modello di Dsu che tiene conto degli approfondimenti e delle indicazioni suggerite dall'Ufficio, anche nel corso di riunioni di lavoro e contatti informali, al competente ufficio del Ministero volti a perfezionare il testo e a renderlo conforme alla disciplina in materia di protezione dei dati personali, in relazione alle operazioni di raccolta delle informazioni relative al nucleo familiare di appartenenza del beneficiario di una prestazione sociale, nonché di consegna da parte degli enti legittimati dell'attestazione dell'Isee, del contenuto della Dsu e di eventuali ulteriori informazioni comunque necessarie al calcolo dell'Isee. Su tali basi, in particolare, l'informativa è stata formalmente inserita nella parte iniziale del modello. Inoltre, è stato precisato che le informazioni indicate nella Dsu come facoltative perseguono finalità di

accesso a determinate prestazioni sociali ovvero di contatto con il dichiarante. Infine, è stato evidenziato all'interno dell'informativa che i controlli sulle informazioni rese dal dichiarante avranno ad oggetto anche i dati personali dei componenti il nucleo familiare. Con riferimento alle modalità per rendere le Dsu disponibili ai dichiaranti è stato specificato che questi ultimi possono eventualmente conferire mandato ai soggetti incaricati della ricezione della Dsu (centri di assistenza fiscale o enti erogatori) a ricevere, ai soli fini del rilascio ai dichiaranti stessi, l'attestazione contenente l'Isee e le altre informazioni usate per il calcolo e, in tal caso, richiedere contestualmente all'Inps di rendere disponibili le medesime informazioni e attestazioni.

Il parere del 12 giugno 2014, n. 295 (doc. web n. 3255963) è invece dedicato al sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp), articolato sistema informativo istituito presso l'Inail (ora Inps) che coinvolge più archivi informativi riferibili a diversi soggetti istituzionali contenente, tra l'altro, dati sensibili dei lavoratori (cfr. par. 3.4.1).

**Sinp**

### 4.3. *L'accesso ai documenti amministrativi*

L'Autorità è frequentemente chiamata ad intervenire sulle tematiche riguardanti l'accesso ai documenti amministrativi (sovente a seguito del mancato riscontro, oppure del diniego di accesso opposto dalle amministrazioni, non di rado adducendo generici rinvii alla disciplina in materia di protezione dei dati personali) e sulla presunta violazione di norme sul relativo procedimento amministrativo. In tali occasioni l'Ufficio ha ribadito che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60 del Codice), le quali attribuiscono il diritto di prendere visione e di estrarre copia di documenti amministrativi ai soggetti 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). In questi casi, infatti, spetta all'amministrazione destinataria dell'istanza entrare nel merito ed accertare l'eventuale qualificata posizione di pretesa all'informazione del richiedente. Inoltre, le valutazioni in ordine alle determinazioni assunte sull'accesso esulano dall'ambito di competenza di questa Autorità e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990, come modificata dalla l. n. 15/2005) (note 2 e 17 settembre 2014 nonché 19 novembre 2014).

In tale contesto, appare utile evidenziare una segnalazione relativa alla produzione, in allegato a una denuncia, di atti e documenti contenenti dati personali asseritamente acquisiti in modo illecito presso un comune; pur non essendo stata accertata l'acquisizione degli atti in violazione dei presupposti di legittimità previsti dalla legge, l'Ufficio ha ricordato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali eventualmente non conforme a disposizioni di legge o di regolamento, restano comunque disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale e che spetta al giudice, ove ritualmente richiesto, valutare la liceità del trattamento dei dati personali dell'interessato (art. 160, comma 6, del Codice) (nota 25 novembre 2014).

Su richiesta del Ministero delle politiche agricole, alimentari e forestali, l'Autorità è stata inoltre chiamata ad esprimere le proprie valutazioni in ordine ai rapporti tra l'accesso difensivo ai sensi dell'art. 24, comma 7, l. 7 agosto 1990, n. 241 e le dispo-

sizioni preclusive previste dagli artt. 2, 3 e 4, d.m. 5 settembre 1997, n. 392, che individua le categorie di atti sottratti all'accesso presso il predetto Ministero. In proposito, è stato evidenziato che su tali questioni il Garante ha adottato un provvedimento di carattere generale (cfr. provv. 9 luglio 2003, doc. web n. 29832) sui diritti di cd. pari rango nel quale si forniscono specifiche indicazioni sulla valutazione che le amministrazioni sono tenute ad effettuare in relazione ai diversi diritti in gioco (nota 5 marzo 2014).

**Vitalizi**

La Regione Lombardia ha interpellato l'Autorità in ordine alla possibilità di pubblicare sul sito istituzionale i nominativi dei consiglieri percettori di assegno vitalizio, con specificazione degli importi, della decorrenza e del complessivo ammontare dei contributi versati, nonché di rilasciare tale documentazione ad un giornalista che l'aveva richiesta, ai sensi della l. n. 241/1990, unitamente all'elenco dei consiglieri della trascorsa legislatura che avevano optato per il riscatto dei contributi e di quelli che avevano optato per i vitalizi. L'Ufficio, nel ribadire la piena vigenza delle norme in materia di accesso ai documenti amministrativi (artt. 59 e 60), ha evidenziato che tali disposizioni, non avendo inciso in modo restrittivo sulla normativa posta a salvaguardia della trasparenza amministrativa, non possono essere invocate per negare, in via di principio, l'accesso ai documenti. Inoltre, nel caso in cui 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" (cfr. nota 6 maggio 2004, doc. web n. 1007634). Tale precisazione, rivolta a chi utilizza la documentazione a cui ha avuto legittimamente accesso per l'esercizio dell'attività giornalistica, costituisce un'applicazione dei principi generali dettati dal Codice per i trattamenti svolti in ambito giornalistico (cfr. art. 137 e All. A.1 al Codice) (nota 3 febbraio 2014).

**Accesso dei consiglieri comunali**

Sono state sottoposte all'attenzione del Garante anche numerose problematiche riguardanti l'accesso di consiglieri comunali agli atti degli enti locali di appartenenza.

Al quesito sulla legittimità di consentire l'accesso al protocollo mediante l'estrazione di copia dei documenti riferiti al singolo numero di protocollo attraverso apposita richiesta scritta, oppure se fosse legittimo consentire la consultazione diretta del predetto registro mediante il rilascio di apposite credenziali di accesso, l'Ufficio, oltre a richiamare la giurisprudenza amministrativa sul punto ed i provvedimenti di carattere generale già emanati (cfr., tra gli altri, nota 20 maggio 1998, doc. web n. 40979; comunicato stampa 9 giugno 1998, doc. web n. 48924; parere 10 giugno 1998, doc. web n. 39348; nota 8 giugno 1999, doc. web n. 40369; nota 8 febbraio 2001, doc. web n. 1075036; nota 4 aprile 2001, doc. web n. 42070; provv. 14 luglio 2005, doc. web n. 1157675, e da ultimo provv. 25 luglio 2013, n. 369, doc. web n. 2604062), ha evidenziato la piena vigenza della norma che riconosce ai consiglieri comunali e provinciali il "diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato" (art. 43, comma 2, d.lgs. 18 agosto 2000, n. 267). Quanto all'individuazione delle notizie e informazioni utili alle quali può essere consentito l'accesso, deve farsi riferimento a tutti gli atti che possano essere effettivamente utili allo svolgimento dei compiti del consigliere e alla sua partecipazione alla vita politico-amministrativa dell'ente. Ciò al fine di permettere di valutare, con piena cognizione, la correttezza e l'efficacia dell'operato dell'amministrazione nonché per esprimere un voto consapevole sulle questioni di competenza del Consiglio e per promuovere le iniziative che spettano ai singoli rappresentanti del corpo elettorale locale (cfr., ad es., C.d.S., Sez. V, 17 settem-

bre 2010, n. 6963). Spetta, pertanto, all'Amministrazione entrare nel merito della valutazione della richiesta ed accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* del consigliere comunale, valutazione eventualmente sindacabile dal giudice amministrativo. La finalizzazione dell'accesso all'espletamento del mandato costituisce il presupposto che legittima l'accesso e che, al tempo stesso, ne delimita la portata (nota 3 aprile 2014).

Altre fattispecie hanno riguardato eventuali limiti all'accesso dei consiglieri comunali laddove le informazioni contenute nella documentazione rivestano particolare delicatezza, come nel caso di una richiesta concernente l'accesso alla relazione integrale dell'assistente sociale contenente dati sensibili, oppure a documentazione contenuta nel fascicolo relativo ad un minore in carico ai servizi sociali del comune, contenente dati sensibili riferiti allo stesso. Al riguardo è stato evidenziato che, nell'ipotesi in cui l'accesso dei consiglieri comunali riguardi dati sensibili, l'esercizio di tale diritto, ai sensi dell'art. 65, comma 4, lett. *b*), del Codice, è consentito in quanto 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 è espressa positivamente con parere del 21 settembre 2005, doc. web n. 1170239; cfr. anche provv. 25 luglio 2013, n. 369, doc. web n. 2604062). I dati personali eventualmente acquisiti devono essere 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 (ad es. art. 22, comma 8, del Codice che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (note 12 marzo e 4 settembre 2014).

### 4.4. *La trasparenza amministrativa*

Per quanto riguarda il tema della trasparenza e della pubblicazione in internet di dati personali, a seguito dell'entrata in vigore del d.lgs. n. 33/2013 e considerate le numerose istanze ricevute, il Garante ha adottato le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (provv. 15 maggio 2014, n. 243, doc. web n. 3134436: in merito v. pure par. 13.3).

Le nuove Linee guida sono state elaborate tenuto conto delle osservazioni e dei riscontri ricevuti dal Dipartimento della funzione pubblica, dall'Autorità nazionale anticorruzione e per la valutazione e la trasparenza delle amministrazioni pubbliche (già Civit e ora Anac) e dall'AgID ed hanno sostituito le precedenti "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" (provv. 2 marzo 2011, n. 88, doc. web n. 1793203).

Il Garante ha, in primo luogo, sottolineato che rimane ferma la regola generale per la quale i soggetti pubblici possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge o di regolamento (art. 19, comma 3, del Codice).

In tal quadro, è necessario distinguere fra obblighi di pubblicazione *online* di dati per finalità di trasparenza oppure per altre finalità della p.a. (ad es., albo pretorio o altre forme di pubblicità dichiarativa, notizia o integrativa dell'efficacia) cui si applicano le indicazioni contenute, rispettivamente, nella prima e nella seconda parte delle Linee guida.