L'attività svolta dal Garante

PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le pubbliche amministrazioni

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

Nel 2013 il Garante ha espresso parere favorevole sullo schema tipo aggiornato di regolamento per il trattamento di dati sensibili e giudiziari presso i consigli e le assemblee legislative delle Regioni e delle Province autonome (provv. 25 luglio 2013, n. 370, doc. web n. 2576905). La revisione dello schema tipo è stato frutto di un complesso e proficuo lavoro di collaborazione dell'Autorità con la Conferenza dei presidenti delle assemblee legislative delle Regioni e delle Province autonome. Il nuovo testo, predisposto dalla Conferenza, tiene conto della necessità di adeguare i regolamenti regionali sul trattamento di dati sensibili e giudiziari al mutato quadro normativo in vari settori di attività di competenza dei consigli e delle assemblee legislative.

A tale proposito, come è noto, il Codice prevede che, per poter trattare dati sensibili e giudiziari indispensabili allo svolgimento delle attività istituzionali, le Regioni e le Province autonome – non diversamente dagli altri soggetti pubblici – debbano dotarsi di specifici regolamenti volti a individuare quali informazioni vengono utilizzate, per quali finalità e mediante quali operazioni di trattamento (artt. 20 e 21 del Codice).

Al riguardo, sin dal 2005 il Garante ha intrapreso un'attività di collaborazione con la Conferenza dei presidenti delle assemblee legislative delle Regioni e delle Province autonome che ha condotto, in un primo tempo, all'elaborazione di un primo schema tipo di regolamento, sul quale l'Autorità ha espresso un parere condizionato al rispetto di alcune indicazioni (provv. 29 dicembre 2005, doc. web n. 1210939), successivamente modificato ed integrato (in merito cfr. il parere condizionato adottato con provv. 12 giugno 2008, doc. web n. 1537639); nel corso del 2013 è stato poi approntato uno schema tipo aggiornato di regolamento che ha tenuto conto degli approfondimenti e delle indicazioni suggeriti dall'Ufficio in via collaborativa, volti a perfezionare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali: le osservazioni formulate hanno riguardato, tra l'altro, il rispetto dei principi di pertinenza e non eccedenza nel trattamento dei dati sensibili di titolari di incarichi politici e di vertice, nonché di incarichi dirigenziali, di collaborazione e di consulenza in attuazione degli obblighi di pubblicazione previsti dalla disciplina in materia di trasparenza e di contrasto della corruzione; le cautele da adottare nel trattamento delle informazioni sulla vita sessuale delle persone soggette a misure restrittive della libertà personale da parte dai Garanti regionali per i diritti dei detenuti; i limiti da rispettare nell'utilizzo di dati sensibili e giudiziari di terzi nell'ambito delle attività di sindacato ispettivo, di indirizzo politico e di documentazione dell'attività istituzionale dei consigli e delle assemblee legislative.

Ciononostante, nell'esprimere il parere, l'Autorità ha chiesto l'integrazione dello schema con la previsione di specifiche garanzie in tema di accesso dei consiglieri regio-

nali a documenti amministrativi; in particolare, il Garante ha richiesto di specificare che le istanze di accesso ai documenti da parte dei consiglieri possano essere accolte solo se riconducibili alle "esclusive" finalità di rilevante interesse pubblico "direttamente connesse all'espletamento di un mandato elettivo" (art. 65, comma 4, del Codice) e che possano essere soddisfatte soltanto con modalità tali da assicurare che l'accesso del consigliere comporti il minor pregiudizio possibile alla vita privata delle persone cui si riferiscono i dati contenuti nei documenti oggetto dell'istanza di accesso. Ciò anche al fine di garantire che il diritto di accesso in questione sia esercitato con riguardo ai dati effettivamente utili per l'esercizio del mandato, fermo restando che i dati personali eventualmente acquisiti dal consigliere possono essere utilizzati per le sole finalità realmente pertinenti al mandato (cfr. provv. 25 luglio 2013, n. 369, doc. web n. 2536172, illustrato *infra* par. 4.3).

4.2. *Le grandi banche dati pubbliche*

Linee guida AgID (art. 58, comma 2, del Cad)

Il Garante ha espresso parere favorevole sulle linee guida redatte dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'art. 58, comma 2, d.lgs. 7 marzo 2005, n. 82 (Cad), il quale 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 (provv. 4 luglio 2013, n. 332, doc. web n. 2574977).

Nell'aprile 2011, DigitPA, ora AgID, aveva pubblicato una prima versione delle predette linee guida in relazione alle quali, in collaborazione con l'Ufficio, erano state apportate modifiche e integrazioni volte, in particolare, a migliorare gli aspetti relativi alle convenzioni aventi per oggetto l'accesso a dati personali e a rendere conformi alla disciplina in materia di protezione dei dati personali i trattamenti ivi previsti.

Il testo, modificato nel 2013, oltre a prevedere il necessario rispetto delle misure minime di sicurezza previste dal Codice (art. 33), reca anche le misure necessarie prescritte dal Garante ai destinatari delle linee guida ("erogatore" e "fruitore" dei dati) al fine di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento (art. 31 del Codice), salvo che le convenzioni medesime o le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti.

In caso di convenzioni già stipulate ai sensi del predetto art. 58, comma 2, del Cad, anteriormente all'adozione delle nuove linee guida, le misure necessarie individuate nel provvedimento dovranno essere adottate in occasione del rinnovo delle stesse e, comunque, entro e non oltre il 30 giugno 2014.

Il Garante ha ritenuto altresì necessario che l'AgID segnali all'Autorità le difformità relative agli aspetti di sicurezza e protezione dei dati personali rilevate nell'ambito dei controlli effettuati dall'Agenzia stessa sulle convenzioni-quadro e metta a disposizione del Garante, per via telematica, un documento aggiornato contenente i dati relativi alle convenzioni, al fine di agevolare le procedure di controllo dell'Autorità, anche in coordinamento con la medesima Agenzia.

Le misure necessarie prescritte dal Garante hanno riguardato, in particolare, le modalità d'accesso e gli aspetti di protezione dei dati personali, individuando anche accorgimenti volti ad assicurare la correttezza del trattamento e a ridurre rischi nell'utilizzo dei dati personali, con specifica attenzione ai presupposti per l'accesso alle

banche dati verificandone periodicamente la base normativa, le finalità istituzionali perseguite dal fruitore, la natura e la qualità dei dati richiesti. Deve essere inoltre prescelta la modalità telematica di accesso alle banche dati più idonea rispetto alle caratteristiche anche infrastrutturali e organizzative del fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso, offrendo – nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore – un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., *web service* che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione).

Per la cooperazione applicativa, viene specificato che i *web service* devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalità istituzionali per le quali è consentita la comunicazione delle informazioni contenute nella banca dati. In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore vengano esclusivamente integrati con il proprio sistema informativo e che non siano resi disponibili a terzi per via informatica.

Oltre a garantire il rispetto delle misure minime di sicurezza previste dagli artt. 33 e ss. del Codice, e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice, per quanto riguarda la fruibilità dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare, in particolare, che gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete *Ip* dell'ente autorizzato e/o dotate di certificazione digitale in modo che sia identificata univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali).

Inoltre, i sistemi *software*, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui *server* che sulle postazioni di lavoro e, in caso di accessi via web, deve essere di regola esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse.

Tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono poi essere adeguatamente tracciate e il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; codice che, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque univocamente riferito al singolo utente incaricato del trattamento che ha dato origine alla transazione.

L'erogatore e il fruitore devono predisporre idonee procedure di *audit* sugli accessi alle banche dati basate sul monitoraggio statistico delle transazioni e su meccanismi di *alert* che individuino comportamenti anomali o a rischio, i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es., numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

È comunque compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad es., delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o del volume di trasferimenti).

Banca nazionale dei contratti pubblici

Il Garante ha espresso parere favorevole sulle modifiche alla deliberazione n. 111/2012 dell'Autorità per la Vigilanza sui Contratti Pubblici (AVCP) concernente il trattamento dei dati nell'ambito della Banca nazionale dei contratti pubblici (parere 1° agosto 2013, n. 377, doc. web n. 2576925).

Le modifiche, finalizzate ad agevolare le stazioni appaltanti nel porre in essere gli adempimenti previsti dal Codice, hanno riguardato, in particolare, l'utilizzo della CEC-PAC (Comunicazione Elettronica Certificata – Pubblica Amministrazione Cittadino) e di caselle di posta ordinaria opportunamente configurate e con specifiche cautele di gestione che sostituiscano la Pec personale unicamente fino al termine del regime facoltativo di utilizzo del sistema AVCpass (previsto per il 31 dicembre 2013).

Il Garante ha inoltre verificato che l'AVCP, valutato quanto prescritto nel precedente parere del 19 dicembre 2012, n. 420 (doc. web n. 2171106), ha individuato il termine di sei mesi per la conservazione dei dati relativi agli accessi e alle operazioni compiute sul sistema AVCpass.

Accessi abusivi

Hanno altresì formato oggetto d'esame segnalazioni relative ad accessi abusivi al sistema informativo dell'Inps che, a seguito di accertamenti di carattere ispettivo svolti anche in collaborazione con il Nucleo della Guardia di finanza, hanno portato alla segnalazione dei fatti alle competenti Procure della Repubblica.

Gli estratti contributivi dei segnalanti erano stati acquisiti dal sistema informativo dell'Inps attraverso utenze regolarmente rilasciate dall'Istituto a soggetti, operanti presso patronati convenzionati, che avevano fatto accesso ai dati personali dei segnalanti in assenza della prescritta delega (note 15 e 22 ottobre 2013).

Inoltre, su segnalazione dell'Inps e di alcuni privati, l'Autorità ha collaborato con la Polizia postale in relazione ad un caso molto grave concernente innumerevoli accessi a banche dati pubbliche, compreso il sistema informativo dell'Istituto (nota 22 ottobre 2013). Al riguardo si è potuto presumere l'utilizzo illegittimo di credenziali assegnate ad operatori di patronato, riscontrando un elevato numero di connessioni al predetto sistema informativo originate da singoli indirizzi *Ip* con modalità di interrogazione compatibili con l'utilizzo di cd. robot per estrarre i dati. Le indagini di polizia giudiziaria, poste in essere dal Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), hanno così permesso di porre fine ad un illecito servizio *online* realizzato utilizzando abusivamente le credenziali assegnate agli operatori di patronato per ricavare posizioni previdenziali e contributive. In particolare, una società è risultata offrire a pagamento tale servizio sul proprio sito web, a soggetti interessati all'accesso ad informazioni patrimoniali (in particolare, professionisti o società finanziarie), anche attraverso un sistema di ricariche prepagate.

Con riferimento, invece, ad una segnalazione relativa ad un presunto accesso abusivo all'Anagrafe tributaria, l'Ufficio ha richiesto all'Agenzia delle entrate di verificare eventuali accessi non autorizzati ai dati personali del segnalante. In seguito all'intervento dell'Autorità, l'Agenzia, dopo aver effettuato un'attività di tracciamento degli accessi avvenuti sui propri sistemi informativi, ha compiuto una complessa attività di *audit* all'esito della quale sono emerse condotte valutabili dal punto di vista penale che sono state comunicate, a cura della stessa Agenzia, alla Procura della Repubblica per le attività di competenza (nota 25 luglio 2013).

Anagrafe nazionale degli abilitati alla guida

Con provvedimento del 24 gennaio 2013, n. 25 (doc. web n. 2256617), del quale si è dato conto nella Relazione annuale 2012 (p. 73), il Garante aveva prescritto al Ministero delle infrastrutture e dei trasporti che, a partire dalla data del provvedimento, le comunicazioni agli interessati – anche nella forma della consultazione diretta tramite il cd. portale dell'automobilista – relative alle variazioni di punteggio della patente (decurtazioni e attribuzioni di punti) avrebbero dovuto contenere i dati relativi alla totalità delle variazioni dei punti della patente, ancor-

ché effettuate in modo automatizzato, ivi comprese l'attribuzione di punti che, successivamente, si rivelasse non legittimamente effettuata, in modo da rendere conoscibile all'interessato la relativa operazione di annullamento. Con riferimento agli eventi passati, il Garante aveva altresì prescritto che, su richiesta dell'interessato, avrebbe dovuto essere assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazioni di punteggio della patente.

In data 8 agosto 2013, il Ministero delle infrastrutture e dei trasporti ha fornito riscontro alle richieste formulate dal Garante nel citato provvedimento, comunicando di aver adeguato le procedure informatiche del sistema informativo per conformarsi alle sopramenzionate prescrizioni dell'Autorità.

4.3. *L'accesso ai documenti amministrativi*

Le tematiche riguardanti l'accesso ai documenti amministrativi continuano ad essere oggetto di intervento dell'Autorità a causa delle numerose segnalazioni e richieste di chiarimenti presentate sia dalle pp.aa., sia dai singoli. Tra le questioni più rilevanti, si registra il caso in cui il Garante ha riscontrato l'illiceità del trattamento dei dati personali effettuato in una Regione nella quale si è consentita la messa a disposizione e consultazione, da parte di alcuni dirigenti, del fascicolo personale di un dipendente – peraltro contenente dati idonei a rivelarne lo stato di salute – in violazione degli artt. 11, comma 1, lett. *d*), 20, commi 1 e 2, e 22, commi 3 e 5, del Codice (provv. 24 ottobre 2013, n. 469, doc. web n. 2799174).

L'Ufficio è stato nuovamente interessato da quesiti relativi alla possibilità di rendere ostensibile a testate giornalistiche documentazione in possesso dell'amministrazione. In particolare, il Servizio bilancio, contabilità, provveditorato ed assistenza al collegio dei revisori dei conti di un Consiglio regionale ha chiesto di pronunciarsi sulla istanza formulata da una testata giornalistica televisiva volta ad ottenere informazioni circa l'erogazione delle indennità a un consigliere regionale. In merito, è stato ribadito che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60) e che "i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla l. 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso" (art. 59, comma 1). Per tale motivo, le valutazioni relative alle determinazioni assunte dall'amministrazione interpellata aventi ad oggetto le richieste di accesso ai documenti esulano dall'ambito di competenza del Garante e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990).

In ordine, poi, alle eventuali richieste di accesso formulate dagli organi di stampa, la disciplina in materia di protezione dei dati personali – non avendo inciso in modo restrittivo sulla normativa posta a salvaguardia della trasparenza amministrativa – non può essere invocata per negare, in via di principio, l'accesso ai documenti. Di conseguenza, rimane "affidata alla responsabilità del giornalista l'utilizzazione lecita del dato raccolto e quindi la sua diffusione secondo i parametri dell'essenzialità rispetto al fatto d'interesse pubblico narrato, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo". Tale indicazione – contenuta già nei chiarimenti del Garante del 6 maggio 2004 (doc. web n. 1007634) – è rivolta a chi, nell'esercizio dell'attività giornalistica, utilizza la documentazione a cui ha avuto legittimamente accesso e costituisce un'applicazione dei principi generali già dettati

dal Codice (cfr. in particolare l'art. 137) nonché dalle disposizioni del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (Allegato A.1 al Codice) (nota 23 settembre 2013).

Accesso dei consiglieri regionali

Sul bilanciamento tra il diritto dei consiglieri regionali ad accedere alle informazioni utili all'espletamento del loro mandato e il diritto alla riservatezza, in particolare quando la richiesta di accesso riguarda documentazione sanitaria riferita a terze persone, è intervenuto il Garante a seguito delle segnalazioni di due amministrazioni regionali destinatarie di istanze di accesso a certificati medici e cartelle cliniche per verificare la correttezza dei servizi erogati dagli organi sanitari regionali (provv. 25 luglio 2013, n. 369, doc. web n. 2536172).

Nel primo caso, il Presidente di un Consiglio regionale aveva chiesto di conoscere i nominativi del personale medico e infermieristico giudicato inabile a svolgere alcune mansioni presso Asl, aziende e presidi ospedalieri del Servizio sanitario regionale nonché di visionare le copie delle certificazioni di invalidità e di verificare la composizione degli organi di accertamento dello stato invalidante. Nel secondo caso, un consigliere regionale aveva formulato istanza di accesso ad una Asl con riguardo alla cartella clinica di un paziente sottoposto a trattamento sanitario obbligatorio (Tso) per effettuare delle verifiche.

A tale proposito, il Garante ha richiamato la disciplina sul trattamento di dati sensibili effettuato da soggetti pubblici, che considera di rilevante interesse pubblico il trattamento delle sole informazioni indispensabili per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo, quale, appunto, quello dei consiglieri regionali (art. 65, comma 4, lett. *b*), del Codice).

Su tale base, l'Autorità ha sottolineato come il diritto di accesso a dati sensibili da parte dei consiglieri regionali incontri un limite nel rispetto dei principi di indispensabilità e di diretta riconducibilità alla funzione perseguita (artt. 20 e 22 del Codice), precisando che l'osservanza di tali principi deve essere particolarmente accurato quando l'istanza ha ad oggetto, come nei casi segnalati, documentazione sanitaria, riferita a persone identificate o identificabili, in relazione alla quale l'ordinamento prevede un particolare regime di tutela, oltre ai comuni obblighi di rispetto del segreto professionale del medico.

La protezione dei dati di carattere personale, con particolare riferimento a quelli attinenti alla salute, gioca infatti un ruolo fondamentale per l'esercizio del diritto al rispetto della vita privata e familiare garantito dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Come ha rilevato la Corte europea dei diritti dell'uomo, il rispetto del carattere confidenziale delle informazioni idonee a rivelare lo stato di salute costituisce un principio essenziale del sistema giuridico di tutti i Paesi europei aderenti alla Convenzione; ciò non soltanto al fine di proteggere la vita privata dei pazienti, ma anche di salvaguardare la fiducia generale nei confronti del personale medico e dei servizi sanitari in generale (cfr. Corte EDU, *Z v. Finland*, sentenza 25 febbraio 1997).

Pertanto, seppure tra i compiti affidati all'Autorità non rientra quello di autorizzare o negare l'accesso ai documenti amministrativi, il Garante ha ritenuto opportuno precisare, in relazione alle peculiari vicende prospettate, che le richieste avanzate dai consiglieri regionali possono essere soddisfatte attraverso modalità che assicurino che l'esercizio delle attività di controllo nell'espletamento del mandato del consigliere avvenga, in concreto, in modo da comportare il minor pregiudizio possibile alla vita privata delle persone interessate. Ciò anche al fine di garantire che il diritto di accesso sia esercitato con riguardo ai dati effettivamente utili per l'esercizio del mandato e ai fini di questo, fermo restando che i dati personali eventualmente acquisiti dal consigliere possono essere utilizzati per le sole finalità pertinenti al mandato.

Tornando quindi ai casi sopra richiamati, nel primo l'Autorità ha prescritto che il Presidente del Consiglio regionale possa accedere alle informazioni richieste solo previo oscuramento dei nominativi del personale giudicato inabile a svolgere alcune mansioni. Nel secondo, il Garante ha disposto che il consigliere regionale istante possa accedere alla cartella clinica del paziente sottoposto a Tso solo dopo avere interpellato la persona interessata (o il suo legale rappresentante) al fine di consentire all'interessato di opporsi per motivi legittimi al trattamento di informazioni che lo riguardano (art. 7, comma 4, del Codice).

Sulle misure prescritte alle due Regioni il Garante ha ritenuto opportuno acquisire il previo parere della Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei Ministri.

Anche le problematiche riguardanti l'accesso di consiglieri comunali agli atti degli enti locali di appartenenza sono state sottoposte all'attenzione dell'Autorità da una società trasporto passeggeri e da un comune. Sul punto è stato ricordato che il Garante ha sempre evidenziato la piena vigenza della specifica disposizione di legge 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). Anche in tal caso, la disciplina di riferimento demanda al soggetto interpellato – che non deve chiedere alcun consenso agli interessati (artt. 24, comma 1, lett. *a*), del Codice), né alcuna autorizzazione all'Autorità – l'obbligo di accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* dei consiglieri degli enti locali interessati, nel rispetto dei limiti e delle condizioni stabilite dalla richiamata normativa di settore (art. 43, comma 2, d.lgs. n. 267/2000) (note 28 maggio e 5 novembre 2013).

4.4. *La trasparenza amministrativa*

Per quanto riguarda il tema della trasparenza e della pubblicazione su internet di informazioni personali sono pervenute numerose istanze in ordine al corretto trattamento dei dati personali contenuti in atti e delibere diffusi sui siti web di organi istituzionali statali nonché di regioni ed enti locali.

In proposito il Garante aveva già adottato le "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" (provv. 2 marzo 2011, n. 88, doc. web n. 1793203). Tali linee guida – attualmente in fase di revisione e aggiornamento a seguito dell'entrata in vigore del d.lgs. 14 marzo 2013, n. 33, in relazione al quale il Garante ha, come detto, reso un proprio parere (provv. 7 febbraio 2013, n. 49, doc. web n. 2243168, sul quale v. *supra* par. 3.2.2) – individuavano un primo quadro unitario di misure e accorgimenti destinati a tutte le pp.aa. che effettuano, in attuazione alle disposizioni normative vigenti, attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli.

Diffusione di dati relativi a Tso

Sul tema, si evidenzia la condotta, tenuta da 27 comuni e segnalata dalla Guardia di finanza, consistente nella pubblicazione delle ordinanze del sindaco sui siti istituzionali nelle quali, riportando in chiaro i dati identificativi e la patologia sofferta dai soggetti sottoposti a trattamento sanitario obbligatorio (Tso) (ed in molti casi indicizzando i predetti dati nei principali motori di ricerca generalisti), si autorizzavano i menzionati trattamenti sanitari. In tali fattispecie è stato rilevato che l'art. 22, comma

8, del Codice prevede che nel trattamento effettuato da soggetti pubblici i "dati idonei a rivelare lo stato di salute non possono essere diffusi" (cfr., in tal senso, anche l'art. 65, comma 5, e l'art. 68, comma 3, del Codice) e che, pertanto, è vietata la diffusione di dati da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Per questa ragione, è stata vietata l'ulteriore diffusione su internet di tali dati prescrivendo ai comuni di attivarsi presso i responsabili dei principali motori di ricerca, al fine di sollecitare la rimozione delle copie web delle ordinanze di Tso dagli indici e dalla *cache* dei motori di ricerca [cfr. provv.ti 3 ottobre 2013, n. 432 (doc. web n. 2747962); 4 aprile 2013, n. 160 (doc. web n. 2488234), n. 159 (doc. web n. 2473879), n. 158 (doc. web n. 2460997), n. 157 (doc. web n. 2452536), n. 156 (doc. web n. 2448446), n. 155 (doc. web n. 2433468), n. 154 (doc. web n. 2427771); 21 marzo 2013, n. 140 (doc. web n. 2389232), n. 137 (doc. web n. 2390451), n. 139 (doc. web n. 2390632), n. 138 (doc. web n. 2390488); 14 marzo 2013, n. 121 (doc. web n. 2389148), n. 120 (doc. web n. 2388972), n. 119 (doc. web n. 2388608), n. 118 (doc. web n. 2388550), n. 117 (doc. web n. 2388358); 7 marzo 2013, n. 102 (doc. web n. 2352966), n. 101 (doc. web n. 2350940), n. 100 (doc. web n. 2343470), n. 99 (doc. web n. 2324649), n. 98 (doc. web n. 2324625), n. 97 (doc. web n. 2322279), n. 96 (doc. web n. 2322248), n. 95 (doc. web n. 2322211), n. 94 (doc. web n. 2322055), n. 93 (doc. web n. 2322036); 21 febbraio 2013, n. 76 (doc. web n. 2358792), n. 75 (doc. web n. 2355041)].

Analogo provvedimento è stato adottato nei confronti di un comune (provv. 3 ottobre 2013, n. 432, doc. web n. 2747962) che aveva pubblicato una determinazione dirigenziale avente ad oggetto la concessione di un beneficio economico a un malato, indicando in chiaro la patologia nonché i dati anagrafici (nominativo, luogo e data di nascita) dell'interessato e del proprio "familiare referente" (comprensivi del codice fiscale e del numero Iban su cui accreditare le somme). Anche in questa circostanza, è stato rilevato che i soggetti pubblici non possono diffondere dati idonei a rivelare lo stato di salute (artt. 22, comma 8, 65, comma 5 e 68, comma 3, del Codice), vietando, come nel caso precedente, l'ulteriore diffusione dei dati sul web e prescrivendo la rimozione della copia web della predetta determinazione dirigenziale dagli indici nonché dalla *cache* dei motori di ricerca.

Sempre in materia di trasparenza, si segnalano alcuni interventi funzionali a richiamare l'attenzione sulla necessità che la diffusione di dati personali sia sempre prevista da idonei presupposti normativi. Si richiamano, a titolo esemplificativo, le segnalazioni ricevute in ordine al trattamento effettuato da due comuni che hanno proceduto alla pubblicazione dei dati dei bambini ammessi (e non) al servizio di trasporto scolastico, con indicazione del nominativo di ciascuno e di ulteriori informazioni (quali il codice fiscale, il numero di linea del mezzo utilizzato, l'orario di partenza e di ritorno), lasciando peraltro che i nominativi fossero indicizzabili dai motori di ricerca. L'Ufficio ha ritenuto tali condotte non conformi al Codice attesa l'assenza di idonei presupposti normativi per la diffusione (art. 19, comma 3, del Codice) (note 10 aprile e 21 novembre 2013).

Albo pretorio *online*

Continuano a pervenire segnalazioni relative alla diffusione di dati personali sull'albo pretorio *online* degli enti locali o di altri soggetti pubblici rispetto alle quali si è più volte riscontrata una condotta non conforme alla disciplina in materia di dati personali per la mancanza di un idoneo presupposto normativo per la pubblicazione oppure in ragione della persistente diffusione dei dati personali sul web oltre il periodo previsto per l'affissione all'albo (ad es., quindici giorni per l'albo pretorio; cfr. artt. 19, comma 3, del Codice e 124, d.lgs. 18 agosto 2000, n. 267) (note 5 gennaio e 19 aprile 2013).

Sanzioni amministrative su siti istituzionali

Si segnalano inoltre alcuni interventi sulla questione della pubblicazione sui siti web istituzionali dei comuni dei nomi dei soggetti destinatari di sanzioni amministrative. Al riguardo, l'Ufficio ha ritenuto che la pubblicazione dei dati personali degli autori di illeciti amministrativi costituisca una sanzione accessoria che, in quanto tale, può essere prevista solo da una legge. In base alla normativa di settore e come ribadito dalla costante giurisprudenza di legittimità, infatti, anche per le sanzioni amministrative accessorie è necessario rispettare il principio di legalità alla luce del quale "nessuno può essere assoggettato a sanzioni amministrative se non in forza di una legge che sia entrata in vigore prima della commissione della violazione" (art. 1, comma 1, l. 24 novembre 1981 n. 689; cfr., *ex plurimis*, Corte cost. 5 aprile 2012, n. 82) (nota 24 aprile 2013).

Sulla medesima questione è stata ritenuta illecita la pubblicazione sul sito web istituzionale di un comune dei verbali di violazione del codice della strada contenenti dati personali, in quanto priva di un idoneo presupposto normativo (art. 19, comma 3, del Codice) (nota 22 luglio 2013).

4.5. *La documentazione anagrafica e la materia elettorale*

Nel periodo di riferimento, la materia anagrafica ed elettorale è stata oggetto di attenzione da parte dell'Autorità.

Liste elettorali

Nel caso di una richiesta di chiarimenti da parte di alcuni comuni in ordine alla legittimità del rilascio di copia delle liste elettorali ad associazioni (anche onlus), l'Ufficio ha precisato che la normativa di settore ammette il rilascio di elenchi degli iscritti nell'Anagrafe della popolazione residente solamente verso le pp.aa. "che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", mentre il rilascio di dati anagrafici a privati può essere disposto dall'ufficiale di anagrafe solo se si tratta di dati "resi anonimi e aggregati" e per "fini statistici e di ricerca" (art. 34, commi 1 e 2, d.P.R. 30 maggio 1989 n. 223). A tali comuni è stata pertanto richiamata la normativa di settore che, invece, prevede che le "liste elettorali possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso" (art. 177, comma 5, del Codice, che ha sostituito l'art. 51, comma 5, d.P.R. 20 marzo 1967, n. 223) (note 29 aprile e 28 maggio 2013).

Elenchi anagrafici

Un altro caso ha riguardato la richiesta, formulata da un dipartimento di sanità pubblica del Servizio sanitario regionale, volta ad acquisire elenchi e vari dati anagrafici relativi a cittadini residenti in 74 comuni della regione, allo scopo di realizzare un progetto volto a migliorare le conoscenze relative agli aspetti ambientali e a valutarne l'impatto sulla salute dei cittadini (Progetto "Supersito" – Regione Emilia Romagna). A mente di quanto previsto dall'art. 19, comma 2, del Codice, l'Ufficio ha richiamato la disciplina di settore che prevede il rilascio alle pp.aa. di elenchi di iscritti all'Anagrafe "per esclusivo uso di pubblica utilità", nonché di dati "resi anonimi ed aggregati, agli interessati che ne facciano richiesta per fini statistici e di ricerca" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223); è inoltre previsto il rilascio di "dari anagrafici, resi anonimi ed aggregati, agli interessati che ne facciano richiesta per fini statistici e di ricerca" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223). Nel caso di specie, il Garante ha precisato che i trattamenti che il Dipartimento di sanità pubblica del Servizio sanitario regionale, in collaborazione con l'Agenzia regionale per la protezione ambientale (Arpa), andava ad effettuare, ove finalizzati alla ricerca scientifica in campo medico, bio-

medico o epidemiologico (in particolare, con dati già raccolti presso strutture sanitarie o esercenti le professioni sanitarie per fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca) avrebbero dovuto essere conformi alle specifiche disposizioni sulla ricerca scientifica in campo medico, biomedico ed epidemiologico (artt. 106 e 110 del Codice; Allegato A.4, codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, doc. web n. 1556635; autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica, del 1° marzo 2012, n. 85, doc. web n. 1878276). Ove, invece, i medesimi trattamenti fossero preordinati al perseguimento di finalità amministrative correlate ai compiti del Servizio sanitario, avrebbe dovuto essere rispettato il quadro generale di garanzie previsto dalla legislazione in materia di trattamento di dati sensibili e dallo specifico regolamento regionale adottato in conformità allo schema tipo (sul quale il Garante ha espresso parere favorevole con provvedimento del 13 aprile 2006, doc. web n. 1272225) (nota 17 dicembre 2013).

Certificati *online*

Si segnala altresì il caso di un cittadino che aveva lamentato l'attivazione, sul sito web istituzionale del proprio comune di residenza, del servizio *online* attraverso il quale era possibile scaricare certificati (fra gli altri, di residenza, cittadinanza, nascita, esistenza in vita, stato civile, godimento dei diritti politici, iscrizione nelle liste elettorali, matrimonio, stato di famiglia) senza alcun tipo di autenticazione o accesso selezionato, ma inserendo semplicemente il codice fiscale dell'interessato. L'Ufficio ha richiesto informazioni al Dipartimento per gli affari interni e territoriali presso il Ministero dell'interno, il quale ha evidenziato, tra l'altro, che l'Agenzia per l'Italia Digitale, interpellata al riguardo, si era espressa nel senso che, ai sensi dell'art. 64, d.lgs. 7 marzo 2005, n. 82 (Cad), ai fini dell'identificazione *online*, l'inserimento del solo codice fiscale non rientra tra gli "strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi" (*ex* comma 2 dell'art. 64 cit.) utili all'individuazione del soggetto richiedente il servizio. È stato inoltre rappresentato che la soluzione tecnologica "timbro digitale" per l'autenticazione delle certificazioni anagrafiche e di stato civile, autorizzata dallo stesso Ministero dell'interno in via sperimentale in alcuni comuni, prevede che la richiesta, da parte del cittadino, della certificazione avvenga previa autenticazione informatica e riconoscimento "con CIE/CBNS e *user id-password* per i servizi richiesti da web". In tale quadro, pertanto, il comune in questione è stato invitato a voler tenere in considerazione le corrette modalità, così individuate, per consentire l'accesso ai predetti certificati in conformità alla disciplina di settore (nota 5 luglio 2013).

Anagrafe elettorale

In tema di anagrafe elettorale dei soggetti residenti all'estero l'Ufficio è intervenuto per fornire informazioni in merito alla cancellazione di un nominativo dalle liste elettorali della circoscrizione consolare estera di residenza. In proposito, è stato rappresentato che la normativa di settore stabilisce che "sono iscritti di ufficio nelle liste elettorali i cittadini che, possedendo i requisiti per essere elettori e non essendo incorsi nella perdita definitiva o temporanea del diritto elettorale attivo, sono compresi nell'Anagrafe della popolazione residente nel comune o nell'Anagrafe degli italiani residenti all'estero (Aire)" (art. 4, d.P.R. 20 marzo 1967, n. 223) e che "sono elettori tutti i cittadini italiani che abbiano compiuto il diciottesimo anno di età" salvo eccezioni previste dalla legge (cfr., in particolare, artt. 1 e 2 del decreto citato); disposizioni normative puntuali disciplinano espressamente, inoltre, le ipotesi di rettifica e revisione delle liste elettorali (cfr., in particolare, artt. 20 e 32 del decreto citato). È stato pertanto chiarito che, al di fuori delle ipotesi che la normativa di settore ha preso in considerazione, non è possibile ottenere la cancellazione del proprio nominativo dalle liste elettorali (nota 10 settembre 2013).

Aire

Analogamente, con riferimento alla segnalazione di un cittadino relativa alla ricezione di un messaggio di propaganda elettorale al proprio indirizzo di residenza all'estero, è stato evidenziato che, già con il provvedimento del 7 settembre 2005 (doc. web n. 1165613) – richiamato dal provvedimento del 10 gennaio 2013, n. 1 (doc. web n. 2181429) –, per attività di propaganda elettorale sono utilizzabili senza consenso i dati contenuti "nelle liste elettorali che ciascun comune tiene, aggiorna costantemente e rilascia in copia anche su supporto elettronico" nonché l'"elenco aggiornato dei cittadini italiani residenti all'estero finalizzato a predisporre le liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (Aire) e degli schedari consolari". In merito, la specifica normativa di settore prevede che "Il Governo, mediante unificazione dei dati dell'anagrafe degli italiani residenti all'estero e degli schedari consolari, provvede a realizzare l'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle lisre elettorali" (art. 5, comma 1, l. n. 459/2001) e che nell'elenco aggiornato dei cittadini italiani residenti all'estero di cui all'art. 5, comma 1, l. n. 459/2001, "sono registrati i seguenti dati: nome e cognome del cittadino italiano, cognome del coniuge per le donne coniugate o vedove, luogo e data di nascita, sesso, stato di residenza, inditizzo, casella postale, ufficio consolare, comune di isctizione all'anagrafe degli italiani residenti all'estero" (art. 5, comma 1, d.P.R. 2 aprile 2003, n. 104). La medesima normativa prevede altresì che "dopo la realizzazione dell'elenco aggiornato con le modalità di cui al presente articolo, il Ministero dell'interno comunica in via informatica al Ministero degli affari esteri, entro il sessantesimo giorno antecedente la data delle votazioni in Italia, l'elenco provvisorio dei residenti all'estero aventi diritto al voto, ai fini della successiva distribuzione in via informatica agli uffici consolari per gli adempimenti previsti dalla legge" (art. 5, comma 8, d.P.R. n. 104/2003). Alla luce di tali elementi, non sono stati ravvisati gli estremi per promuovere l'adozione di un provvedimento del Garante (nota 29 maggio 2013).

Sotto un diverso profilo, il Dipartimento per gli affari interni e territoriali presso il Ministero dell'interno (nota 31 maggio 2013) ha informato l'Autorità di aver pienamente aderito all'orientamento da questa espresso (nota 29 agosto 2012, in Relazione 2012, p. 77) in ordine ad una richiesta presentata da Ancitel s.p.a. di ottenere copia delle liste elettorali in qualità di responsabile del trattamento designata da taluni enti *non profit*, che agiscono quali titolari del trattamento per finalità comprese tra quelle previste dalle vigenti disposizioni in materia (art. 51, comma 5, d.P.R. n. 223/1967, come modificato dall'art. 177, comma 5, del Codice). Nella richiesta era previsto che i predetti dati sarebbero stati successivamente trasmessi per l'elaborazione a Consodata s.p.a., anch'essa designata responsabile e da questa consegnati ai suddetti enti. A tal proposito è stato rappresentato dall'Ufficio che le organizzazioni non lucrative, legittimate ad ottenere dai comuni il rilascio di copia delle liste elettorali e ad utilizzarle per il perseguimento delle finalità individuate dalla normativa vigente, possono richiedere a soggetti esterni (nel caso di specie Ancitel s.p.a. e Consodata s.p.a.) lo svolgimento di specifiche operazioni di trattamento. I dati, però, non possono essere comunicati ad altri titolari e possono essere utilizzati solo per le finalità perseguite dagli enti titolari del trattamento riconducibili a quelle tassativamente individuate dal citato art. 51, comma 5, d.P.R. n. 223/1967.

In prossimità delle consultazioni elettorali tenute nel mese di febbraio 2013 per le elezioni dei consigli regionali delle Regioni Lombardia e Molise nonché per le consultazioni tenute a maggio per le elezioni dei sindaci, dei consigli comunali nonché dei consigli circoscrizionali, e per le consultazioni tenute nel mese di giugno per l'elezione del Presidente e del Consiglio regionale della Regione Autonoma Valle d'Aosta, l'Autorità ha approvato alcuni provvedimenti (provv.ti 10 gennaio 2013,

n. 1, doc. web n. 2181429; 24 aprile 2013, n. 228, doc. web n. 2404305) che confermano le prescrizioni già stabilite dal provvedimento generale del 7 settembre 2005 (doc. web n. 1165613), prevedendo speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati in relazione all'uso dei dati personali a fini di comunicazione politica e di propaganda elettorale. Il citato provvedimento del 24 aprile 2013, n. 228, ha ribadito che i cittadini devono essere sempre informati sull'uso effettuato dei loro dati. Tuttavia, partiti, movimenti politici, sostenitori e singoli candidati sono stati esonerati dal predetto obbligo di informativa sino al 31 agosto 2013 solo per i dati raccolti da registri ed elenchi pubblici, e utilizzati per l'invio di materiale propagandistico di dimensioni così ridotte da non consentire di inserirvi una informativa, anche sintetica. Trascorso tale termine il Garante ha altresì previsto che i medesimi soggetti devono fornire agli interessati un'idonea informativa entro il 31 ottobre 2013 o altrimenti cancellare le informazioni personali. È stato altresì rappresentato che, alla luce del quadro normativo successivo alle modifiche all'art. 130 del Codice e della istituzione del "Registro pubblico delle opposizioni" (art. 13, comma 3, del Codice; d.P.R. 7 settembre 2010, n. 178), per i trattamenti effettuati per l'inoltro di messaggi elettorali e politici è necessario il consenso informato degli intestatari di utenze pubblicate negli elenchi telefonici; è stata inoltre ribadita la necessità del consenso degli interessati per talune modalità di comunicazione (in particolare per l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore, nonché mediante dispositivi quali, ad es., posta elettronica, telefax, messaggi del tipo mms o sms), come previsto dall'art. 130, commi 1 e 2, del Codice.

4.6. *L'istruzione scolastica ed universitaria*

Anche nel 2013 l'Autorità è intervenuta fornendo chiarimenti in relazione al trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica ed universitaria.

In particolare, una scuola ha posto un quesito circa la necessità di acquisire la preventiva autorizzazione del Garante al fine di poter istituire un "ambiente di apprendimento" *online* con servizi disponibili per gli studenti. Al riguardo, l'Ufficio, nel precisare che, salvo i casi espressamente previsti, i trattamenti di dati personali non devono essere previamente autorizzati dal Garante, ha ribadito il dovere di rispettare la disciplina in materia di protezione dei dati personali, evidenziando, in particolare, la necessità di sottoporre a verifica preliminare i trattamenti che presentano specifici rischi per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare (artt. 17, 40 e 41 del Codice; nota 25 giugno 2013).

È stata segnalata una presunta violazione della disciplina in materia di dati personali presso una scuola superiore di secondo grado in relazione alla somministrazione agli alunni di un test nominativo riguardante una ricerca promossa dal Dipartimento di psicologia dell'Università di Firenze, effettuata senza fornire preventivamente l'informativa sul trattamento dei dati personali (art. 13 del Codice). A seguito dell'intervento dell'Ufficio, il dirigente scolastico ha garantito di aver proceduto alla distruzione dei test compilati dagli studenti, dopo averli messi in sicurezza al fine di impedirne l'accesso a chiunque (ivi compresi i ricercatori dell'Università), e di aver successivamente consentito la somministrazione del test solo dopo che fosse stata fornita idonea informativa agli studenti. Considerate le garanzie e le idonee assicurazioni fornite, volte ad evitare la ripetizione per il futuro della condotta lamentata, e salva la veri-

fica dei presupposti per la contestazione di eventuali sanzioni amministrative, non sono state intraprese iniziative per l'adozione di provvedimenti da parte del Garante (nota 30 maggio 2013).

È giunta all'Autorità una segnalazione con la quale veniva rappresentato che, ai fini dell'iscrizione all'asilo nido di un comune, venivano raccolti dati personali ritenuti eccedenti e non pertinenti. In particolare, attraverso la modulistica predisposta per l'iscrizione, si richiedeva una pluralità di informazioni inerenti: "il motivo di assenza di uno dei genitori dal nucleo familiare, la presenza di un procedimento di affido o adozione in corso, l'origine straniera di uno o entrambi i genitori, con l'indicazione dell'anno di ingresso in Italia, la professione o la scuola frequentata da altri figli componenti il nucleo familiare, il nome, il cognome, la data di nascita, la residenza dei nonni del minore e se risultano residenti nel territorio del comune, anche l'occupazione, ivi compreso l'orario settimanale di lavoro, lo stato di salute e l'invalidità". L'Ufficio ha potuto accertare che, in base al regolamento comunale, le domande per l'iscrizione all'asilo nido contenenti le informazioni richieste relative alle "situazioni particolari che caratterizzano il nucleo familiare" concernevano esclusivamente la presenza di uno o più componenti con invalidità certificata ai sensi della legislazione vigente, superiore al 67% nonché del nucleo familiare in situazione di fragilità in carico ai servizi sociali. Su tali basi, rilevato il disallineamento tra la più ampia rosa di dati personali richiesti dal comune e quelli effettivamente necessari per verificare la sussistenza dei requisiti di ammissione all'asilo nido, il Garante ha ritenuto indebita l'acquisizione dei dati personali eccedenti. L'Autorità ha, pertanto, vietato al comune la raccolta ed il successivo trattamento dei predetti dati personali nonché di ogni altra informazione non rilevante ai fini della verifica dei criteri previsti nel regolamento comunale, in quanto ciò avrebbe comportato un trattamento di dati personali eccedenti, non pertinenti e, con specifico riferimento ai dati sensibili, non indispensabili rispetto alle finalità perseguite (provv. 6 giugno 2013, n. 273, doc. web n. 2554925).

Comunicazione ai sensi dell'art. 39 del Codice

Una provincia aveva richiesto, ai sensi dell'art. 39 del Codice, al Ministero dell'istruzione, dell'università e della ricerca i dati relativi ai codici fiscali degli studenti della scuola secondaria della provincia "frequentanti, trasferiti, ritirati, bocciati, *etc.*, del primo e ultimo anno di corso, con riferimento agli anni 2012/2013 e 2013/2014", per lo svolgimento delle proprie funzioni istituzionali inerenti la vigilanza sull'assolvimento dell'obbligo scolastico e la realizzazione di un progetto di contrasto alla dispersione scolastica (art. 68, l. 17 maggio 1999, n. 144 e D.G.R. 1891 del 22 giugno 2011). Sul punto l'Ufficio ha preliminarmente evidenziato che il Codice dispone, in via generale, che i soggetti pubblici possano comunicare dati personali, diversi da quelli sensibili e giudiziari, solo se tale specifica operazione di trattamento sia prevista da una norma di legge o di regolamento (cfr. art. 19, comma 3). Inoltre, come ipotesi residuale, in mancanza di una specifica norma di legge o di regolamento che lo preveda, le amministrazioni pubbliche possono comunicare ad altri soggetti pubblici dati personali, non aventi natura sensibile, allorquando tale trattamento sia necessario per lo svolgimento delle proprie funzioni istituzionali. Le amministrazioni coinvolte nel flusso di dati che si intende attivare devono, pertanto, preliminarmente ed attentamente accertare che tale flusso di dati non sia già previsto dalla specifica normativa di settore. In tal caso, il titolare è tenuto ad effettuare una comunicazione preventiva al Garante e il trattamento potrà avere inizio decorsi quarantacinque giorni della predetta comunicazione, salva diversa determinazione anche successiva dell'Autorità (artt. 18, comma 2, 19, comma 2 e 39 del Codice). Su tali basi, rilevata la sussistenza di specifiche disposizioni di regolamento che espressamente disciplinano il flusso di dati necessari alla provincia per l'assolvimento delle funzioni istituzionali concernenti l'obbligo di frequenza di attività formative fino al diciottesimo anno di età e di preven-

zione e contrasto alla dispersione scolastica, l'Ufficio ha ritenuto che le comunicazioni di dati personali per le predette finalità possano avvenire solo nei limiti previsti dalla disciplina di settore (art. 3, commi 2, 3, 4, e 5, e art. 8, comma 2, d.P.R. 12 luglio 2000, n. 257; art. 3, comma 2, d.m. 5 agosto 2010, n. 74 e punto 3 sezione "profilo D" dell'allegato tecnico al d.m. n. 74/2010 cit.) (nota 27 febbraio 2013).

Similmente, il Ministero dell'istruzione, dell'università e della ricerca (Miur) ha comunicato all'Autorità, ai sensi degli artt. 19, comma 2 e 39, comma 2, del Codice, di aver ricevuto da parte di un comune la richiesta dei dati relativi agli alunni iscritti dal 2007 alle scuole di ogni ordine e grado della provincia di appartenenza (nome, cognome, data e luogo di nascita, scuola frequentata ed anno di frequenza) per il perseguimento della funzione istituzionale di partecipazione al contrasto all'evasione fiscale, con particolare riferimento all'accertamento delle residenze fittizie all'estero attraverso la vigilanza sui soggetti che hanno richiesto l'iscrizione all'Aire (in particolare, art. 44, d.P.R. 29 settembre 1973, n. 600 e ss. mm. e art. 83, commi 16 e 17, d. l. 25 giugno 2008, n. 112, convertito dalla l. 6 agosto 2008, n. 133 e ss. mm.).

Al riguardo, l'Ufficio ha rilevato che la normativa di settore stabilisce specifiche regole per il reperimento da parte dei comuni delle informazioni necessarie per la partecipazione al contrasto all'evasione fiscale (cfr. art. 1, d.l. 30 settembre 2005, n. 203 convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248 e modificato dall'art. 18, d.l. 31 maggio 2010, n. 78, convertito dalla l. 30 luglio 2010, n. 122; provvedimenti del Direttore dell'Agenzia delle entrate del 3 dicembre 2007 e del 26 novembre 2008; art. 44, d.P.R. n. 600/1973; art. 83, commi 16 e 17, d.l. n. 112/2008). Tenuto conto della citata normativa, l'Ufficio ha ritenuto quindi non applicabile la disciplina prevista dagli artt. 19, comma 2 e 39, comma 2, del Codice (cfr. in particolare, i citati artt. 44, d.P.R. n. 600/1973 e 83, d.l. n. 112/2008) (nota 21 maggio 2013).

Relativamente al settore universitario, una studentessa ha segnalato all'Autorità che, presso l'Università degli Studi di Roma la Sapienza, attraverso un sistema informatico, ogni docente, inserendo le proprie credenziali, poteva visionare i dati personali di qualunque studente iscritto. L'Università, nel confermare il contenuto della segnalazione, ha messo a punto specifiche soluzioni operative in base alle quali, in particolare, "a partire dall'anno accademico 2013/2014, tutte le carriere degli studenti iscritti ai corsi [...] porranno essere visualizzate da docente sul predetto sistema informatico [...] solo ed esclusivamente nel caso che lo studente si sia già iscritto a sostenere l'esame di profitto di competenza; relativamente alle carriere, ad esaurimento, dei vecchi ordinamenti, per le quali non sono attivi filtri automarici di controllo sul piano di studio, è possibile sviluppare una nuova funzione del sistema [...] che consenta allo studente di autorizzare l'accesso ai propri dati di carriera ai docenti con i quali intenda sostenere esami di profitto; in tal modo ogni docente potrà accedere esclusivamente alle carriere che sono di pertinenza della propria attività istituzionale". Sulla base di tali specifiche assicurazioni l'Ufficio, salva la verifica dei presupposti per la contestazione di eventuali sanzioni amministrative, non ha promosso l'adozione di specifici provvedimenti da parte del Garante (nota 5 aprile 2013).

4.7. *L'attività fiscale e tributaria*

Redditometro

L'Agenzia ha richiesto al Garante una verifica preliminare sul trattamento di dati personali che intendeva effettuare ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, d.P.R. 29 settembre 1973, n. 600 (il nuovo cd. redditometro), modificato dall'art. 22, d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122.