Con provvedimento 17 dicembre 2015, il Garante ha espresso parere favorevole sullo schema di decreto recante le modalità tecniche di emissione della Carta di identità elettronica (Cie), che sostituirà il precedente d.m. 8 novembre 2007, sul cui schema il Garante si era espresso in data 2 agosto 2007. La nuova disciplina è volta a incrementare i livelli di sicurezza del sistema di emissione della Cie attraverso la centralizzazione del processo di produzione e rilascio e l'adeguamento delle caratteristiche agli *standard* internazionali di sicurezza in materia di documenti elettronici (ICAO 9303), già adottati per il permesso di soggiorno e il passaporto elettronici. Il nuovo processo di emissione e produzione della Cie è centralizzato presso il Ministero dell'interno. I comuni ed i consolati acquisiscono i dati identificativi e biometrici del richiedente, mediante postazioni installate dall'Istituto poligrafico e Zecca dello Stato (IpZS), e li inviano, dopo la certificazione dei dati presso il Centro nazionale dei servizi demografici (Cnsd), all'IpZS per la personalizzazione e stampa del documento elettronico. È stata inoltre istituita una Commissione interministeriale per supportare il Ministero dell'interno nella definizione del piano di attuazione presso comuni e consolati, con particolare riferimento alle modalità di adozione degli *standard* tecnologici, alle specifiche tecniche ed eventuali funzionalità aggiuntive, profili sui quali deve essere sentito il Garante.

Le osservazioni allo schema proposto hanno riguardato alcuni aspetti tecnici e misure di sicurezza, la necessità di estendere i casi in cui il Garante deve essere sentito dalla Commissione interministeriale, l'esigenza di coordinare le prescrizioni tecniche previste per la raccolta e la trasmissione del consenso o del diniego alla donazione di organi o tessuti in caso di morte al "Sistema Informativo Trapianti", con quelle previste dalle recenti Linee guida adottate in materia dal Ministero della salute (v. *supra*) secondo i princìpi della cooperazione applicativa (provv. 17 dicembre 2015, n. 656, doc. web n. 4634495).

Il Ministero degli esteri ha richiesto il parere del Garante in ordine alla possibilità, per gli uffici consolari, di rilasciare ai candidati alle elezioni dei Comitati degli italiani all'estero (Comites) i dati dei cittadini residenti all'estero che hanno richiesto di essere iscritti nell'elenco elettorale per partecipare alla consultazione (art. 1, d.l. n. 67 del 30 maggio 2012, come modificato dall'art. 10, comma 3, d.l. n. 109 del 1 agosto 2014, conv., con mod., dalla l. n. 141, 1° ottobre 2014). In base alla normativa, alle elezioni dei Comites, che si svolgono per corrispondenza, sono ammessi al voto solo gli elettori che abbiano fatto pervenire all'ufficio consolare la domanda di iscrizione nell'elenco elettorale almeno trenta giorni prima della data stabilita. Il Ministero degli esteri ha chiesto, se a fronte delle richieste da parte di candidati, scaduto il predetto termine, sia possibile rilasciare l'elenco contenente i dati personali dei cittadini residenti all'estero che hanno fatto domanda di iscrizione al voto (cd. opzione). La richiesta si fonda sulla prospettata esigenza dei candidati di escludere dalla propaganda elettorale coloro che, non avendo esercitato l'opzione, abbiano implicitamente manifestato la volontà di non essere raggiunti da comunicazioni relative a questo evento elettorale. Il Garante, con provvedimento 19 marzo 2015 (n. 165, doc. web n. 3871667), ha ritenuto che l'elenco degli elettori in parola possa essere messo a disposizione dei candidati "per finalità politico-elettorali stabilite dalla legge" (art. 11, comma 3, d.P.R. n. 395/2003), essendo finalizzato allo svolgimento delle operazioni connesse alla gestione del procedimento elettorale, in conformità a quanto già affermato con provvedimento 6 marzo 2014 (n. 107, doc. web n. 3013267).

In risposta alla richiesta di un Comune relativa alla possibilità di rilasciare le liste elettorali ad un parronato che intende utilizzarle, oltre che per finalità di carattere socio-assistenziale e per il perseguimento di un interesse diffuso, anche "per fini strettamente legati alla campagna elettorale", l'Ufficio ha ricordato che le liste elet-

torali possono essere rilasciate in copia solo "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". Ha inoltre, rappresentato che, in base all'orientamento espresso dal Ministero dell'interno, ritenuto condivisibile dall'Autorità, le finalità che legittimano il rilascio delle liste elettorali devono risultare – oltre che motivate ai sensi dell'art. 51, d.P.R. n. 223/1957 – proprie del richiedente e "... ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività di tale organismo...". Pertanto, il Comune destinatario dell'istanza di ostensione delle liste elettorali, è tenuto ad entrare nel merito della richiesta per valutare se la specifica finalità del loro successivo utilizzo, dichiarata dal richiedente, sia conforme all'attività svolta dal soggetto medesimo e se rientri effettivamente tra le ipotesi tassativamente individuate dal cit. art. 51, comma 5, d.P.R. n. 223/1957, così come modificato dall'art. 177, comma 5, del Codice (nota 28 agosto 2015).

Un Comune ha inoltre formulato un quesito in merito alla possibilità di rilasciare gli elenchi anagrafici relativi ai nati nel 2001 ad un istituto statale di istruzione secondaria superiore, al fine di invitare le famiglie alla presentazione della propria offerta formativa in occasione di un *open day*. L'Ufficio ha evidenziato che i soggetti pubblici possono comunicare dati personali ad altri soggetti pubblici solo se tale operazione è prevista da una norma di legge o di regolamento (art. 19, comma 2, del Codice). In base alla normativa di settore, gli ufficiali d'anagrafe possono rilasciare gli elenchi degli iscritti contenuti nell'anagrafe della popolazione residente solamente alle pp.aa. "che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", mentre altri soggetti, anche privati, possono ottenere solo dati anagrafici "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). Pertanto, ferma restando la necessità, in capo al Comune, di valutare se l'utilizzo prospettato dal richiedente sia conforme a quanto previsto dal regolamento anagrafico, l'Ufficio ha chiarito che tra i soggetti cui possono essere rilasciati tali elenchi, non sono ricompresi gli istituti scolastici parificati (nota 5 maggio 2015).

A seguito della segnalazione di una cittadina, che aveva ricevuto alcune comunicazioni promozionali da una scuola professionale privata (una s.r.l.), indirizzate alla figlia, è stato accertato che il Comune aveva provveduto alla comunicazione dei dati anagrafici alla predetta società, nella convinzione che la scuola potesse rientrare tra i soggetti pubblici, in virtù dell'accreditamento presso la Regione di riferimento desumibile dalla presenza del logo istituzionale sulla carta intestata. Anche in questo caso, è stato ribadito che il rilascio degli elenchi degli iscritti all'anagrafe della popolazione residente è previsto solo nei confronti delle pp.aa. che ne facciano motivata richiesta per motivi di pubblica utilità, e non anche a soggetti privati, tra i quali deve ricomprendersi l'istituto scolastico privato parificato (art. 34, comma 1, d.P.R. n. 223). Al riguardo, non rilevando l'eventuale accreditamento presso la Regione ai fini della qualificazione pubblicistica del soggetto, il trattamento dei dati personali da parte del Comune è stato ritenuto illecito (nota 4 marzo 2015).

4.5. *L'istruzione scolastica*

Il trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica è stato oggetto di particolare attenzione anche nel 2015.

Con il provvedimento 28 maggio 2015 il Garante ha reso parere favorevole sullo schema di decreto del Ministero dell'istruzione dell'università e delle ricerca (Miur)

recante la Regolamentazione per la realizzazione e consegna della Carta dello studente denominata "IoStudio". Lo schema di decreto ha recepito le indicazioni fornite dall'Ufficio nel corso di numerosi contatti anche informali con i competenti uffici del Miur.

Tale schema prevede che il Ministero, per il tramite delle segreterie scolastiche, attribuisca una Carta, nominativa e idonea ad attestare lo *status* di studente, a tutti i frequentanti le scuole secondarie di secondo grado statali e paritarie. La Carta, utile per il conferimento di agevolazioni e sconti per l'accesso a beni e servizi di natura culturale, per la mobilità nazionale ed internazionale, per l'acquisto di materiale scolastico, è prodotta da un fornitore designato quale responsabile del trattamento, non autorizzato alla conservazione dei dati degli studenti. Essa, inoltre, può essere utilizzata, su richiesta dello studente o di chi ne esercita la potestà genitoriale, altresì come "borsellino elettronico". A tal fine, previa autenticazione sul Portale dello studente, l'interessato è reindirizzato sul portale del fornitore della Carta che, in tal caso in qualità di autonomo titolare del trattamento, effettua la raccolta dei dati necessari per l'espletamento del servizio richiesto (provv. 28 maggio 2015, n. 313, doc. web n. 4070802).

Il Miur ha altresì presentato uno schema di decreto che, in attuazione dell'art. 10, comma 8, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221, prevede l'integrazione dell'Anagrafe nazionale degli studenti (Ans) con i dati relativi agli iscritti alla scuola dell'infanzia.

Lo schema di decreto dispone in particolare che le istituzioni scolastiche dell'infanzia appartenenti al sistema nazionale di istruzione trasmettano un *set* di 10 informazioni anagrafiche relative ai propri frequentanti all'Ans (cfr. art. 3, d.lgs. 15 aprile 2005, n. 76; decreto del Miur 5 agosto 2010, n. 74, sul cui schema il Garante ha fornito il parere di competenza in data 16 giugno 2010, doc. web n. 1734404). Nel fornire parere favorevole, l'Autorità ha richiamato l'attenzione del Ministero e di tutte le amministrazioni interessate sulla circostanza che i dati personali non possono essere trattati per finalità di vigilanza sull'assolvimento dell'obbligo scolastico, non concernendo tale obbligo la scuola dell'infanzia (parere 8 ottobre 2015, n. 522, doc. web n. 4448919).

Il Miur ha inoltre sottoposto al parere del Garante uno schema di regolamento in materia di Trattamento dei dati idonei a rivelare lo stato di disabilità degli alunni censiti nell'Anagrafe nazionale degli studenti. Tale schema regolamentare attua l'art. 13, comma 2-*ter*, d.l. 12 settembre 2013, n. 104, convertito, con modificazioni, dalla l. 8 novembre 2013, n. 128, il quale prevede che "al fine di consentire il costante miglioramento dell'inregrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno, le istituzioni scolastiche trasmettono per via telemarica alla banca dati dell'Anagrafe nazionale degli studenti le diagnosi funzionali di cui al comma 5 dell'art. 12 della l. 5 febbraio 1992, n. 104, prive di elementi identificativi degli alunni". Lo schema di regolamento definisce in particolare i criteri e le modalità di accesso ai dati di natura sensibile, le misure di sicurezza nonché, nell'ambito dell'Ans, la separazione tra la partizione contenenre le diagnosi funzionali e gli altri dati. Comportando la richiamata normativa il trattamento, con l'ausilio di strumenti elettronici, di dati idonei a rivelare lo stato di salute di un ingente numero di soggetti minori di età, l'Ufficio ha fornito ai competenti uffici del Miur diverse indicazioni volte, in particolare, alla più rigorosa applicazione del principio di indispensabilità nell'individuazione del tipo di dati trattati, alla definizione delle finalità di rilevante interesse pubblico perseguite nonché alle misure di sicurezza applicate per prevenire rischi di distruzione, perdita o accessi non consentiti ai predetti dati. L'Autorità ha, quindi, condizionato il proprio

parere favorevole richiedendo che nell'allegato tecnico allo schema di decreto sia individuato un rermine certo e proporzionato per la conservazione dei *file* di *log* relativi alla registrazione degli accessi (parere 15 ottobre 2015, n. 535, doc. web n. 4448995).

A seguito di una segnalazione, è emerso che una comunità montana ha offerto un servizio di ginnastica correttiva ai ragazzi frequentanti le classi seconde della scuola secondaria di primo grado residenti nel comprensorio comunitario. A tal fine, ha proceduto, in assenza di idonea base notmativa e senza rispettare il principio di necessità, alla raccolta presso le scuole di dati personali riferiti agli studenti che sono stati poi comunicati all'Asl territorialmente competente per il controllo medico previsto dal servizio. La predetta Azienda non ha fornito agli interessati alcuna informativa sul trattamento di dati personali effettuato per finalità di cura (art. 76 del Codice). L'Autorità, nel ricevere per il futuro idonee assicurazioni in ordine alle modalirà di realizzazione di iniziative similari, ha raccomandato di prestare particolare attenzione al corretto adempimento degli obblighi imposti dalla normativa in materia di protezione dei dati personali, con particolare rifetimento a quello di fornire idonea informativa agli intetessati, e nelle ipotesi di trattamento per finalità di cura, di acquisire uno specifico consenso da parte degli stessi, nonché di procedere alla designazione degli incaricati e eventualmente anche di responsabili del trattamento (artt. 13, 76, 29 e 30 del Codice) (nota 2 luglio 2015).

4.6. *L'attività fiscale e tributaria*

Dichiarazione precompilata

Nel 2015 il Garante ha affrontato la tematica relativa all'elaborazione della dichiarazione dei redditi da parte dell'Agenzia delle entrate (cd. precompilata) al fine di assicurare il corretto contemperamento tra la rilevante finalità di semplificazione degli adempimenti fiscali e le necessarie garanzie per la protezione dei dati personali anche a tutela dei familiari a carico che non intendono far conoscere le proprie spese al soggetto dichiarante.

Con patere 19 febbraio 2015 l'Autorità si è espressa favorevolmente in merito allo schema di provvedimento del Direttore dell'Agenzia delle entrate con il quale sono state specificate le modalità tecniche di accesso alla dichiarazione precompilata (n. 95, doc. web n. 3741076). L'Agenzia, pertanto, a seguito di numerosi contatti con l'Ufficio, ha posto in essere una serie di misure tecniche e organizzative volte a prevenire accessi indiscriminati o abusivi ai dari dei contribuenti soprattutto per gli accessi in via telematica da parte di sostituti di imposta, caf e professionisti abilitati. È stato previsto, in particolare, che il contribuente in possesso delle credenziali per l'utilizzo dei servizi telematici dell'Agenzia delle entrate possa accedere direttamente alla propria dichiarazione precompilata, mediante le apposite funzionalità rese disponibili nell'area autenticata del medesimo sito dei servizi telematici, ovvero utilizzando le credenziali dispositive rilasciate dall'Inps. In alternativa, il contribuente può conferire apposita delega al proprio sostituto d'imposta, qualora esso presti assistenza fiscale, ovvero ad un caf o ad un professionista abilitato. Più precisamente, i predetti sostituti d'imposta, i caf e i professionisti abilitati ricevono in via telematica (accesso *offline*) dall'Agenzia delle entrate le dichiarazioni precompilate degli assistiti che abbiano conferito apposita delega, formulando una richiesta contenente l'elenco dei codici fiscali di tali contribuenti, con l'indicazione di alcuni dati relativi alla delega ricevuta nonché di alcune informazioni desunte dalla dichiarazione telativa all'anno d'imposta precedente. Inoltre, i caf e i professionisti abilitati, al fine di poter gestire eventuali richieste di assistenza non programmate, possono effettuare,

previa acquisizione della delega, la richiesta di una singola dichiarazione precompilata, che in tal caso viene resa disponibile in tempo reale (accesso via web). Viene previsto, altresì, che la richiesta di accesso alle dichiarazioni precompilate sia preceduta dalla digitazione di un codice di sicurezza *completely automated public turing test to tell computers and humans apart* (captcha), al fine di evitare l'utilizzo di *robot* per l'accesso ai servizi offerti dall'Agenzia.

In tale quadro, l'Agenzia delle entrate, oltre a svolgere controlli sulle deleghe acquisite e sull'accesso alle dichiarazioni precompilate provvede a richiedere, a campione, copia delle deleghe e dei documenti di identità indicati nelle richieste di accesso alle dichiarazioni precompilare. In tal caso, i sostituti d'imposta, i caf e i professionisti abilitati devono trasmettere i suddetti documenti, tramite posta elettronica certificata, entro 48 ore dalla richiesta. Una specifica previsione ha riguardato, inoltre, il diritto del contribuente di visualizzare l'elenco dei soggetti ai quali è stata resa disponibile la propria dichiarazione precompilata avvalendosi di apposite funzionalità, nonché consultando il proprio cassetto fiscale, disponibile nell'area autenticata del sito dei servizi telematici dell'Agenzia delle entrate.

L'Autorità, ha altresì espresso parere favorevole su un altro schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante l'accesso alla dichiarazione precompilata da parte del Corpo della Guardia di finanza attraverso l'utilizzo delle credenziali personali di accesso alla rete intranet della Guardia di finanza, al fine di consentire a ciascuno di essi di accedere alla propria dichiarazione dei redditi precompilata (provv. 2 aprile 2015, n. 194, doc. web n. 3878833).

Spese sanitarie nella dichiarazione precompilata

Con due distinti pareri l'Autorità è intervenuta al fine di assicurare la protezione dei dati personali nell'ambito della raccolta dei dati sulle spese sanitarie sosrenute nel 2015 per la dichiarazione precompilata 2016 (30 luglio 2015, n. 450, doc. web n. 4160058; 30 luglio 2015, n. 451, doc. web n. 4160102).

Il sistema delineato negli atti sottoposti al parere dell'Autorità, uno schema di decreto del Mef e un provvedimento del Direttore dell'Agenzia delle entrate, prevede che gli erogatori di servizi sanitari (medici, ospedali, farmacie e altri presìdi accreditati) inviino al Sistema tessera sanitaria (Sistema TS) i dati relativi alle prestazioni erogate; nella fase successiva il Mef, una volta ricevuti dall'Agenzia delle entrate i codici fiscali dei cittadini che potranno usufruire della dichiarazione precompilata, rende disponibili alla stessa Agenzia i dati sulle spese sanitarie aggregati per tipologia. I dati che il Sistema TS, fornirà all'Agenzia dal 1° marzo di ogni anno sono quelli delle ricevute di pagamento, degli scontrini fiscali relativi alle spese sanitarie effettuate dal contribuente e dal familiare a carico e quelle dei rimborsi erogati. In particolare, tra le spese rientrano i *ticket* per l'acquisto di farmaci (anche omeopatici) e le prestazioni fornite nell'ambito del Ssn, i dispositivi medici con marcatura CE e i servizi erogati dalle farmacie come per esempio il *test* per la glicemia. Inoltre, sono inclusi anche i farmaci per uso veterinario, le prestazioni sanitarie quali la visita medica generica, le spese agevolabili solo a particolari condizioni come le cure termali e altre spese.

In considerazione della delicatezza dei dati trattati, in accordo con il Mef e l'Agenzia delle entrate, il Garante ha individuato specifiche cautele al fine di assicurare un elevato livello di tutela dei diritti nel rispetto dei princìpi di semplificazione ed efficacia. In particolare, fermi restando i diritti garantiti all'interessato dall'art. 7 del Codice (fra i quali, in particolare, il diritto all'opposizione per motivi legittimi), l'assistito può chiedere, a chi eroga il servizio sanitario, di non trasmettere i dati della singola spesa al Mef o, ove già trasmessi, ottenere la cancellazione anche di singole spese. Tale opposizione può essere esercitata autonomamente anche dalle persone fiscalmente a carico, come il coniuge o i figli (maggiori di sedici anni). Per le

spese sostenute a partire dal 1° gennaio 2016, l'assistito può opporsi alla trasmissione dei dati relativi alla singola prestazione al momento dell'erogazione della stessa chiedendo oralmente al medico, o alla struttura sanitaria, l'annotazione dell'opposizione sul documento fiscale. L'informazione di tale opposizione deve essere conservata anche dal medico/struttura sanitaria. Limitatamente all'anno di imposta 2015, nel periodo compreso tra il 1° ottobre 2015 e il 31 gennaio 2016, è stato previsto che l'assistito possa esercitare la propria opposizione richiedendo all'Agenzia delle entrate la cancellazione di una o più macro tipologie di spesa dal Sistema TS via telefono, posta elettronica o direttamente presso gli uffici territoriali dell'Agenzia dell'entrate. In caso di spese documentate per mezzo del cd. scontrino parlante, invece, tale opposizione può essere esercitata non comunicando, al soggetto che emette lo scontrino, il codice fiscale riportato sulla tessera sanitaria. Inoltre, dal 10 febbraio al 9 marzo 2016 e, in seguito, dal 1° al 28 febbraio dell'anno successivo al periodo di imposta di riferimento, accedendo all'area autenticata del sito web dedicato del Sistema TS, (tramite tessera sanitaria TS-CNS oppure utilizzando le credenziali *fisconline* rilasciate dall'Agenzia delle entrate) l'assistito può consultare l'elenco delle spese sanitarie (compresi i farmaci del cd. scontrino parlante) trasmesse e opporsi alla messa a disposizione anche di singole spese all'Agenzia, richiedendone la cancellazione senza ritardo da parte del Sistema TS. Solo i dati trattati dall'Agenzia delle entrate per l'elaborazione della dichiarazione precompilata sono sottoposti a procedura di storicizzazione, al fine di consentire a posteriori le apposite verifiche. I restanti dati saranno cancellati, entro l'anno successivo al periodo di riferimento. Occorre precisare che l'Agenzia delle entrate non può accedere al dettaglio delle singole spese sanitarie degli assistiti, ma solo a dati automaticamente aggregati dal Mef in base alle predefinite macro tipologie di spesa (ad es., *ticket*, farmaco, spese per prestazioni specialistiche). Gli intermediari abilitati (caf e professionisti), previa delega del contribuente, possono accedere unicamente al totale delle spese sanitarie detraibili. In sostanza, quindi, la consultazione in chiaro delle voci relative alle singole spese sanitarie è consentita esclusivamente all'assistito sul sito web del Sistema TS.

Ad ogni buon conto, il Garante ha costituito un tavolo di confronto con il Mef e l'Agenzia delle entrate per valutare migliorie del sistema a garanzia della tutela dei dati personali dei cittadini interessati, soprattutto per quanto riguarda la tutela dei familiari a carico maggiorenni che non intendono far conoscere l'ammontare delle proprie spese mediche al familiare dichiarante.

FATCA

Nel 2015 il Garante ha affrontato la tematica relativa all'attuazione in Italia della normativa in materia di scambio automatico obbligatorio di informazioni nel settore fiscale.

Al riguardo, il Mef ha richiesto un parere all'Autorità in riferimento allo schema di decreto attuativo dell'Accordo tra Italia e USA, ratificato dall'Italia con la l. 18 giugno 2015, n. 95, recante "Ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Governo degli Stati Uniti d'America finalizzato a migliorare la *compliance* fiscale internazionale e ad applicare la normativa FATCA (*Foreign Account Tax Compliance Act*), con Allegati, fatto a Roma il 10 gennaio 2014, nonché disposizioni concernenti gli adempimenti delle istituzioni finanziarie italiane ai fini dell'attuazione dello scambio automatico di informazioni derivanti dal predetto Accordo e da accordi tra l'Italia e altri Stati esteri". L'Accordo prevede che gli istituti finanziari italiani, raccolgano all'atto di apertura di ogni nuovo rapporto successivo al 1° luglio 2014, specifici dati dei clienti cittadini americani o residenti negli USA per comunicarli, poi, all'Agenzia delle entrate che successivamente li trasferirà all'amministrazione fiscale degli Stati Uniti per finalità di contrasto all'e-

vasione fiscale. Il contenuto dello schema ha tenuto conto delle indicazioni rese dall'Autorità all'esito di riunioni e contatti informali con l'amministrazione interessata, volte a completare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali.

Il Garante, nel merito, si è espresso favorevolmente con la raccomandazione di indicare nel preambolo le disposizioni del Codice che rendono lecita la raccolta dei dati da parte degli operatori finanziari e la successiva comunicazione dei dati negli Stati Uniti. In particolare, la raccolta dei dati personali da parte delle predette istituzioni finanziarie è consentita ai sensi dell'art. 24, comma 1, lett. *a*) del Codice, secondo cui un soggetto privato può effettuare un trattamento di dati personali senza il consenso dell'interessato quando sia "necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria". Il trasferimento dei dati all'estero è stato considerato invece necessario per la salvaguardia di un interesse pubblico rilevante (art. 43, comma 1, lett. *c*), da rinvenirsi, nel caso in esame, in quello indicato nell'art. 66 del Codice, in materia tributaria e doganale. È stato altresì richiesto di inserire nel preambolo un richiamo alle disposizioni convenzionali vigenti per ricondurre il trattamento dei dati ad esclusive finalità fiscali e assicurare che le informazioni scambiate possano essere comunicate soltanto alle persone o autorità incaricate dell'accertamento o della riscossione di imposte e delle decisioni di ricorsi al riguardo (provv. 8 luglio 2015, n. 411, doc. web n. 4160287).

L'Autorità ha, inoltre, espresso parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate, parimenti attuativo del predetto Accordo, che disciplina le modalità di trasmissione dei dati ai competenti organi degli Stati Uniti d'America, con particolare riferimento all'idoneità delle misure di sicurezza (parere 23 luglio 2015, n. 438, doc. web n. 4252461).

In materia di comunicazione tra soggetti pubblici di dati personali di carattere fiscale, si segnala la pronuncia della CGUE nel caso Smaranda Bara e a. (sentenza del 1° ottobre 2015, causa C-201/14). Il caso riguardava alcuni cittadini rumeni che contestavano la legittimità, ai sensi della direttiva europea sulla protezione dei dati, della trasmissione delle loro dichiarazioni dei redditi alla Cassa nazionale malattia da parte dell'amministrazione tributaria rumena. Sulla base di tali dichiarazioni, la predetta Cassa nazionale aveva poi richiesto agli interessati il pagamento di contributi previdenziali arretrati. In tale contesto, la Corte ha ritenuto che l'obbligo di trattare lealmente i dati personali (art. 6, direttiva 95/46/CE) richiede che un'amministrazione pubblica informi le persone interessate del fatto che i loro dati saranno trasmessi a un'altra amministrazione che li tratterà in qualità di destinatario. Inoltre, la Corte ha precisato che, sulla base del diritto europeo, ogni eventuale restrizione all'obbligo d'informativa può essere adottata con disposizione legislativa (art. 11, par. 2 direttiva 95/46/CE).

Inoltre, da ultimo, il Garante si è espresso sullo schema di decreto del Mef in materia di scambio automatico obbligatorio di informazioni nel settore fiscale avente per oggetto le regole tecniche per la rilevazione, la trasmissione e la comunicazione all'Agenzia delle entrate, da parte degli operatori finanziari, delle informazioni relative ai cittadini di altri Stati esteri, raccolte in esecuzione di accordi internazionali ai sensi della cit. l. n. 95/2015 (parere 17 dicembre 2015, n. 661, doc. web n. 4634033). In particolare, l'Autorità ha richiamato l'attenzione sulla necessità che siano individuate idonee misure di sicurezza per la raccolta dei dati da parte dell'Agenzia e, una volta trasmesse alle autorità competenti estere, vengano disciplinate le modalità di trattamento da parte dell'Agenzia delle informazioni così raccolte e di quelle che saranno ricevute dalle predette autorità in virtù degli scambi

informativi. Ciò, anche al fine di definire il rapporto esistente tra tali informazioni e quelle dell'archivio dei rapporti finanziari contenuto nell'anagrafe tributaria in termini di garanzie assicurate al trattamento dei dati personali dei contribuenti (cfr. par. 22.3).

Giacenza media dei conti nell'archivio dei rapporti finanziari

A seguito della modifica dell'art. 11, d.l. 6 dicembre 2011, n. 201 da parte della l. 23 dicembre 2014, n. 190, il Garante ha espresso parere favorevole sul provvedimento del Direttore dell'Agenzia delle entrate che disciplina l'integrazione della comunicazione integrativa annuale all'archivio dei rapporti finanziari con la giacenza media relativa ai rapporti di deposito e di conto corrente bancari e postali per la semplificazione degli adempimenti dei cittadini in materia di Isee e per i relativi controlli sulla veridicità dei dati dichiarati dai beneficiari delle prestazioni sociali agevolate. Al riguardo, l'Autorità ha valutato positivamente il fatto che il Ministero del lavoro e delle politiche sociali si sia adoperato con gli istituti bancari e le Poste italiane s.p.a. per rendere più agevole e non oneroso agli interessati il reperimento del valore della giacenza media da parte degli interessati, rilevante ai fini Isee, e che in tal senso si sono prontamente attivati l'Abi e Poste italiane (parere 7 maggio 2015, n. 265, doc. web n. 4038256).

4.7. *La videosorveglianza in ambito pubblico*

Anche nel 2015, il trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico è stato oggetto di grande interesse.

Settore scolastico

In particolare, in relazione al settore scolastico, l'Ufficio ha avuto occasione di ricordare ad un istituto professionale a seguito di un'istanza di un educatore nonché ad un istituto magistrale, che nel provvedimento generale dell'8 aprile 2010 è stata ribadita la necessità di garantire il diritto dello studente alla riservatezza (art. 2, comma 2, d.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo della personalità dei minori in relazione alla loro vita ed al loro diritto all'educazione. È stato, altresì, evidenziato che può risultare ammissibile l'utilizzo di sistemi di videosorveglianza in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate, attivando gli impianti negli orari di chiusura degli istituti e vietando la messa in funzione delle telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola (punto 4.3, provv. 8 aprile 2010, doc. web n. 1712680).

È stato inoltre chiarito che, laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio, evidenziando espressamente che il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (note 15 gennaio e 3 dicembre 2015).

Settore sanitario

Numerosi sono stati i riscontri forniti in relazione a sistemi di videosorveglianza installati in ambito sanitario: in particolare, ad un'Asl, è stato ricordato che nel citato provvedimento generale del 2010 l'Autorità ha evidenziato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti, stante la natura sensibile di molti dati che possono essere raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati. Nel medesimo provvedimento il Garante, nel far presente che devono essere adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e

della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 (doc. web n. 1191411), ha, altresì, evidenziato che il titolare del trattamento deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (ad es., personale medico ed infermieristico) e che devono essere invece previsti, nel caso di reparti dove non sia consentito l'accesso (ad es., rianimazione), adeguati accorgimenti tecnici per limitare la visione dell'immagine, da parte di terzi legittimati (familiari, parenti, conoscenti di ricoverati), solo del proprio congiunto o conoscente. Considerato che le immagini idonee a rivelare lo stato di salute non devono essere diffuse (art. 22, comma 8, del Codice), va evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico; al riguardo, è stato rappresentato che il mancato rispetto delle citate prescrizioni comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (cfr. punto 4.2. del predetto provv. generale). Nella medesima occasione è stata richiamata l'attenzione sulla necessità che il titolare o il responsabile designino per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (art. 30 del Codice); deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (ad es., registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.) (cfr. punto 3.3.2. del cit. provv.).

È stato chiarito, comunque, che non è riconducibile alla protezione dei dati personali né ai compiti demandati all'Autorità la questione relativa alla necessità o meno che i soggetti che gestiscono l'attività di videosorveglianza rivestano la qualifica di guardia giurata. In ogni caso, ove l'Asl intenda avvalersi del contributo di altri soggetti, per lo svolgimento dei propri compiti istituzionali vanno, comunque, osservate le regole ordinarie in merito alla designazione dei responsabili del trattamento (art. 29 del Codice) (nota 17 marzo 2015).

Nel medesimo settore, l'Ufficio ha fornito alcune precisazioni telative ai casi in cui è necessaria la verifica preliminare del Garante: in particolare, un istituto aveva sotroposto a verifica preliminare la possibilità di installare sistemi di videosorveglianza per la tutela dell'incolumità dei lavoratori, per il controllo delle stanze di degenza e per il monitoraggio dei pazienti ricoverati non autosufficienti e portatori di handicap psichico/fisico; ciò, anche al fine di acquisire ogni informazione necessaria in caso di eventi problematici connessi con la gestione dei pazienti o di eventi delittuosi, considerato che il medesimo istituto era stato in passato coinvolto in una indagine di polizia per malttattamenti degli ospiti della struttura da parte di medici e operatoti sanitari. Al riguardo, l'Ufficio nel ricordare le ipotesi in cui i trattamenti di dati personali effettuati tramite videosorveglianza devono essere sottoposti alla verifica preliminare dell'Autorità, ha fatto presente che i ttattamenti prospettati non fossero riconducibili alle predette ipotesi e, pertanto, non occorreva sottopotli alla vetifica preliminate dell'Autorità. In ogni caso, è stato evidenziato che il sistema di videosorveglianza che si intendeva installare sembrava finalizzato non tanto alla tutela dei lavoratori e pazienti, quanto piuttosto alla prevenzione e repressione dei reati, il cui perseguimento compete alle Forze di polizia; è stata, altresì, rammentata la vigente disciplina di settore sull'attività di controllo a distanza dell'attività dei

lavoratori (nota 8 giugno 2015).

Analogamente, ad una cooperativa che aveva formulato una istanza di verifica preliminare per prolungare sino a tre mesi i tempi di conservazione delle immagini registrate dall'impianto di videosorveglianza, con la finalità di tutela dei beni e della salute degli assistititi in relazione a possibili atti di autolesionismo e di aggressione da parte di altri assistititi e conseguente accertamento di responsabilità civili e penali, è stato rappresentato che, poiché compete esclusivamente alle Forze di polizia il perseguimento di finalità di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica, l'istante non poteva installare sistemi di videosorveglianza per il perseguimento di tali finalità (nota 18 dicembre 2015).

Settore trasporto pubblico

Sempre in relazione ad una richiesta di verifica preliminare, l'Ufficio ha risposto ad una istanza di una azienda di trasporti pubblici che intendeva fornire a coloro che verificano i titoli di viaggio, fotocamere o *smartphone* con lo scopo di consentire l'acquisizione delle immagini degli utenti che, trovati sprovvisti di idoneo titolo di viaggio, al momento della verbalizzazione, non avevano fornito spontaneamente un documento di riconoscimento; ciò, al fine di consentire all'azienda di trasporti di contrastare l'evasione tariffaria, garantire la prevenzione e la repressione dei reati ai danni dell'azienda e dei cittadini, aumentando il senso di sicurezza percepita dall'utenza. Al riguardo, nel far presente che la procedura di identificazione prospettata non risultava conforme alle specifiche disposizioni di settore che già compiutamente disciplinano i presupposti e le modalità di identificazione personale (cfr. art. 11, d.l. 21 marzo 1978, n. 59, convertito con modificazioni, dalla l. 18 maggio 1978, n. 191; artt. 357, 496 e 651 c.p.; artt. 4 e 157, r.d. 18 giugno 1931, n. 773), l'azienda è stata invitata a verificare la conformità dell'iniziativa che si intendeva assumere al quadro normativo sopra richiamato (nota 8 ottobre 2015).

Medesime indicazioni in ordine ai presupposti e alle modalità di identificazione personale sono state fornite ad un'altra azienda provinciale dei trasporti che chiedeva se fosse corretta la procedura in base alla quale i soggetti preposti alla verifica dei titoli di viaggio potessero richiedere, a fini identificativi, il numero di telefono cellulare agli utenti sprovvisti di titolo di viaggio, in caso di impossibilità al riconoscimento degli stessi, per mancata esibizione o possesso del documento di riconoscimento (nota 23 ottobre 2015).

È stato, invece, correttamente sottoposto alla verifica preliminare dell'Autorità un sistema di videosorveglianza intelligente installato da un'autorità portuale presso i porti di sua giurisdizione per le finalità di tutela del patrimonio e delle persone che accedono e lavorano nelle aree portuali. Il sistema prospettato risultava abilitato a svolgere la specifica funzione di attivare un allarme sonoro presso la *control room* in caso di attraversamento di una linea virtuale posta in corrispondenza del limite superiore della recinzione metallica, con lo scopo di segnalare l'eventuale scavalcamento da parte di soggetti non autorizzati della recinzione metallica posizionata lungo il perimetro delle aree ad accesso ristretto (riservate, in taluni porti, a dipendenti, fornitori e passeggeri nelle operazioni di imbarco e sbarco e, in un altro, al personale adibito alle operazioni di movimentazione merci); la citata attività di video analisi è stata ritenuta idonea a rilevare automaticamente, segnalare e registrare un comportamento o evento anomalo, quale può considerarsi l'ingresso in aree qualificate "ad accesso ristretto", in cui la limitazione dell'accesso risultasse adeguatamente segnalata con la presenza di idonei cartelli informativi e con dispositivi di delimitazione delle zone costituiti da barriere *new jersey* sormontate da recinzioni a maglie metalliche. Nello specifico, esaminata la normativa di settore, è stato chiarito che l'autorità portuale, per lo svolgimento delle proprie funzioni istituzionali può legittimamente controllare le aree che rientrano nella sua circoscrizione territo-

riale, con particolare riferimento alle zone ad accesso ristretto, anche attraverso l'installazione di sistemi di videosorveglianza (cfr. att. 6, commi 1, lett. *a*), 2 e 8, l. 28 gennaio 1994, n. 84; art. 1, d.P.R. 29 dicembre 2000; artt. 4, comma 1, lett. *f*); 11, comma 1, lett. *b*) e 18, comma 2, del Codice; regolamento del Parlamento europeo e del Consiglio relativo al miglioramento della sicurezza delle navi e degli impianti portuali n. 725/2004; programma nazionale di sicurezza marittima contro eventuali azioni illecite intenzionali approvato con d.m. del Ministero dei trasporti n. 83/T del 2007). Le caratteristiche specifiche del sistema previsto, inoltre, avendo come unico effetto rispetto all'attivazione dell'allarme quello di richiamare l'attenzione dell'operatore della *control room* al fine di consentirgli di verificare la fondatezza della segnalazione (eventualmente anche azionando delle telecamere "dome", per seguire manualmente l'intruso fino all'arrivo delle guardie giurate), non comportavano l'attivazione di ulteriori funzionalità, quali, ad esempio, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali, anche biometrici, o confronto con una campionatura precostituita. È stato, pertanto, ritenuto che il sistema intelligente sottoposto a verifica preliminare non arrecasse, in concreto, un pregiudizio rilevante per gli interessati tale da determinare effetti invasivi sulla loro sfera di autodeterminazione e, conseguentemente, sui loro comportamenti. Il Garante lo ha quindi ritenuto proporzionato e ha accolto la richiesta di verifica preliminare, richiamando l'attenzione sulle prescrizioni relative alle misure di sicurezza, con particolare riferimento alle indicazioni contenute nel citato provvedimento del 2010 (cfr. punto 3.3.1.; artt. 31-36 del Codice e All. B al Codice) (provv. 17 settembre 2015, n. 477, doc. web n. 4361006).

Settore rifiuti

In relazione al trattamento di dati personali effettuato tramite videosorveglianza dai comuni, tra i molteplici riscontri forniti, si segnalano le indicazioni rese ad un Comune abruzzese che aveva formulato un quesito in ordine all'utilizzo di "fototrappole" per monitorare l'abbandono incontrollato di rifiuti nelle zone periferiche del territorio comunale; sul punto, l'Ufficio ha fatto presente che l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose e a monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente, qualora non risulti possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi (art. 13, l. 24 novembre 1981, n. 689) (cfr. punto 5.2., provv. 8 aprile 2010). Nell'ambito degli specifici adempimenti previsti, è stata richiamata l'attenzione sulle indicazioni fornite dall'Autorità in materia di informativa agli interessati in relazione alla quale il Garante ha messo a disposizione modelli semplificati (cfr. punto 3.1. del predetto provv.; art. 13 del Codice) (nota 4 dicembre 2015).

Ad un Comune campano e ad alcuni segnalanti che lamentavano una presunta violazione della normativa in materia di protezione di dati personali derivante dalle modalità di informazione in ordine alla presenza di sistemi di rilevazione automatica degli accessi in una ztl, così come evidenziato nel citato provvedimento del 2010, è stato rappresentato che, nei casi in cui la normativa di settore preveda espressamente l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni, è possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (art. 13, comma 2, del Codice). L'installazione degli avvisi previsti dal codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati per-

sonali e idonei pertanto ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice (punto 5.3.2. del predetto provv. generale) (note 22 settembre e 1° ottobre 2015).

4.8. *I trattamenti effettuati presso regioni ed enti locali*

Raccolta differenziata dei rifiuti solidi urbani

Nel 2015 l'Autorità si è nuovamente occupata, a seguito di istanze di cittadini e di associazioni di consumatori, della tematica relativa al trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti urbani prescelte dai comuni.

In particolare, la questione che ha maggiormente richiesto l'intervento dell'Ufficio ha riguardato l'utilizzo di sacchetti trasparenti per la raccolta differenziata cd. porta a porta, rispetto alla quale, come già negli anni passati, è stata richiamata l'attenzione dei comuni interessati sulla prescrizione contenuta nel provvedimento generale 14 luglio 2005 (doc. web n. 1149822) che considera, in termini generali, non proporzionato l'obbligo di utilizzare un sacchetto trasparente in quanto chiunque si trovi a transitare sul pianerottolo o nell'area antistante l'abitazione può visionare agevolmente il contenuto del sacchetto (cfr. punto 4.a del predetto provv.). In un caso è stato precisato in particolare che i cittadini sono tenuti a utilizzare un mastello chiuso, all'interno del quale depositare i sacchi del rifiuto indifferenziato e che, per utenze con specifiche necessità (ad es., panui e traverse) è possibile rivolgersi ai servizi sociali, per fruire, in forma anonima, di diverse modalità di conferimento quali ad es., i sacchi opachi di colore azzurro (nota 23 gennaio 2015).

Un altro Comune, intetpellato dall'Ufficio, aveva chiarito che la raccolta cd. porta a porta prevedeva che il sacco contenente il rifiuto fosse insetito in appositi contenitori da aprire al momento del ritiro da parte degli operatori (nota 9 gennaio 2015). Infine, un'altra amministrazione comunale, chiamata in causa da numerosi cittadini, aveva dichiarato che i sacchetti previsti per la raccolta di materiali per adulti incontinenti erano in materiale opacizzato e i sacchi per la raccolta di pannolini erano provvisti di *tag*, senza indicare il nome dell'utente, precisando che, in alcune zone periferiche della città, era stata avviata una sostituzione dei sacchetti con bidoni anonimi di diverso colore a seconda della tipologia di rifiuti raccolta (nota 11 marzo 2015).

In un'altra circostanza, invece, l'intervento dell'Ufficio, ha comportato la necessità da parte del Comune interessato di modificare un'ordinanza sindacale, nel senso di eliminare l'obbligo di utilizzare i sacchi trasparenti, consentendo così ai cittadini di conferire i rifiuti in modo che non sia conoscibile il contenuto del sacchetto dall'esterno (nota 21 settembre 2015).

L'istanza di un cittadino ha riguardato un altro aspetto della procedura per la raccolta dei rifiuti ovvero la richiesta, nei confronti dei soggetti conferenti, di esibire un documento di identità al personale preposto alla gestione di apposite aree per il conferimento organizzato dei materiali della raccolta differenziata (cd. piattaforme ecologiche o ecopiazzole), e l'annotazione in un apposito regisrro di nome e indirizzo dei conferenti, della quantità approssimativa del sacchetto nonché del tipo di materiale ricevuto. Al riguardo, è stato rappresentato che alcuni regolamenti comunali prevedono che, nei limiti di una quantità massima giornaliera indicata nel regolamento stesso, in relazione alle diverse tipologie di materiali, i rifiuti siano conferiti senza oneri da parte dei produttori. Nel caso in cui siano superate le quantità indicate per ogni tipologia di rifiuto, il produttore ricorre alla raccolta a domicilio, contattando la società di gestione del servizio, previo pagamento delle spese. In rela-

zione a tale aspetto, deve ritenersi lecito, nei limiti delle finalità istituzionali e ove sia previsto da una disposizione regolamentare (cfr. art. 21, d.lgs. n. 22/1997 ora art. 198, d.lgs. 3 aprile 2006, n. 152), il trattamento dei dati personali (ad es., nome e indirizzo dei conferenti), per la sola finalità di accertamento dell'effettiva residenza nel comune del conferente e per evitare che lo stesso soggetto possa conferire i rifiuti in violazione dei limiti quantitativi ammessi senza oneri a carico dei produttori. Deve essere comunque predisposta un'informativa contenente gli elementi indicati nell'art. 13 del Codice e i dati personali acquisiti devono essere conservati per il solo periodo necessario allo scopo per i quali essi sono stati raccolti (art. 11, comma 1, lett. *d*), (cfr. punto 4.e del predetto provv. generale) (nota 31 dicembre 2015).

Sono state, infine, fornite indicazioni ad un Comune in ordine alla possibilità che ispettori ambientali possano esaminate il contenuto dei sacchetti dei rifiuti, al fine di identificare, attraverso il materiale ispezionato, i presunti trasgressori delle prescrizioni relative alla raccolta differenziata dei rifiuti urbani. In tale circostanza l'Ufficio ha ricordato che agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689), ma tale facoltà deve essere esercitata selettivamente, nei soli casi in cui il soggetto che abbia conferito i rifiuti con modalità difformi da quelle consentite non sia in altro modo identificabile. Risulterebbe, quindi, invasiva la pratica di ispezioni generalizzate da parte del personale incaricato (agenti di polizia municipale; dipendenti di aziende municipalizzate) del contenuto dei sacchetti al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente (cfr. punto 4.d del predetto provv. generale) (nota 10 settembre 2015).

Dati sensibili

Un Comune ha interpellato il Garante in merito alla sottoscrizione di un protocollo d'intesa con un consolato a sostegno delle famiglie e dei minori, in base al quale il Comune si sarebbe impegnato ad informate il consolato sui casi di affidamento di minori, sui provvedimenti adottati dall'autorità giudiziaria in merito a minori allontanati dalla famiglia, nonché adoperato, unitamente al consolato, affinché l'Ambasciatore venisse nominato curatore speciale del minore. Al riguardo, è stato precisato che in base al Codice, la comunicazione preventiva all'Autorità, ai sensi degli artt. 19, comma 2 e 39, comma 1, può essere effettuata solo qualora ricorrano i presupposti concernenti la natura pubblicistica del soggetto destinatario della comunicazione e la tipologia dei dati, diversi da quelli sensibili e giudiziari. Pertanto, nel caso di specie, trattandosi verosimilmente di comunicazione avente ad oggetto dati sensibili e giudiziari, è srato rappresentato che occorre fare riferimento agli artt. 20 e 22 del Codice, nonché al regolamento sul trattamento dei dati sensibili e giudiziari adottato dal Comune (nota 20 luglio 2015).

L'Autorità si è altresì occupata del trattamento, effettuato dal Consiglio regionale della Toscana, dei dati relativi ad erogazioni liberali effettuate volontariamente dai consiglieri regionali a favore di partiti politici. Al riguardo, il Consiglio regionale ha evidenziato di aver ricevuto la richiesta di effettuare una trattenuta volontaria mensile dal cedolino dello stipendio dei consiglieri e di provvedere ad effettuare l'erogazione liberale ai partiti politici indicati dai richiedenti. L'Ufficio ha chiariro che per il trattamento dei dati relativi alle disposizioni di liberalità a favore di partiti politici, trovano applicazione le regole e le garanzie previste per i dati sensibili, in base alle quali il trattamento è ammesso soltanto in base ad "un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite" (artt. 4, comma 1, lett. *d*), 20, 22, del Codice). L'attività sopra descritta, è stata nel frattempo disciplinata dalla l.r. n. 69, 23 ottobre 2015, "Assicurazione pre-

videnziale integrativa e atti di liberalità da attivare su richiesta dei consiglieri e degli assessori regionali. Modifiche alla l.r. 3/2009", che ha previsto che "il consigliere o l'assessore regionale che intenda compiere atti di liberalità, ad esclusione delle donazioni, a favore di soggetti terzi o al fine di acquisire servizi connessi all'esercizio del mandato, può chiedere alla competente struttura del Consiglio regionale di fare da tramite per l'effettuazione della relativa trattenuta e del versamento". Pertanto, in virtù della modifica normativa intervenuta, l'Ufficio ha ritenuto lecita l'attività in parola, qualora effettuata, in conformità alla menzionata normativa, mediante il trattamento delle sole informazioni e delle operazioni strettamente indispensabili previste dal regolamento sul trattamento dei dati sensibili e giudiziari del Consiglio regionale della Toscana, n. 24, 12 febbraio 2014 (scheda n. 4) (nota 10 novembre 2015).

L'Autorità è stata consultata dalla presidenza della Regione Abruzzo in relazione ai trattamenti di dati sensibili connessi all'istituzione di un ufficio di ascolto sociale presso la Regione, al quale cittadini, ma anche gruppi ed associazioni, possono rivolgersi per rappresentare "situazioni personali bisognevoli di attenzioni solidali", al fine di ricercare "iniziative sostenibili per una molteplicità di problematiche scaturenti da difficoltà di carattere sociale" e seguire l'*iter* amministrativo delle vicende prospettate. L'Ufficio ha ritenuto che il regolamento sul trattamento dei dati sensibili e giudiziari della Regione in conformità allo schema tipo, disciplina espressamente i trattamenti dei dati connessi allo svolgimento delle funzioni dell'istituendo ufficio di ascolto sociale (cfr. in particolare la scheda n. 11 allegata al regolamento) (nota 4 marzo 2015).

4.9. *La previdenza e l'assistenza sociale*

Un'associazione Onlus si è rivolta al Garante per una valutazione in merito alla legittimità della richiesta, proveniente dall'Associazione Banco Alimentare del Lazio Onlus (ente capofila), di ottenere la comunicazione delle liste nominative dei propri assistiti e di mettere a disposizione i relativi fascicoli personali, al fine di essere convenzionati con la predetta Associazione capofila e ricevere, per il suo tramite, le risorse alimentari dell'Agenzia per le erogazioni in agricoltura (Agea) da distribuire ai propri assistiti.

L'istruttoria svolta ha evidenziato che l'Agea è l'Organismo intermedio di gestione per l'attuazione del "Programma Operativo sugli aiuti alimentari e l'assistenza materiale" (PO1), per la gestione del quale vengono attinte somme provenienti dal "Fondo di Aiuti Europei agli Indigenti" (FEAD), ai sensi del regolamento (UE) n. 223/2014 del Parlamento Europeo e del Consiglio. Con le "Istruzioni operative n. 22" del 28.8.2014, l'Agea ha fissato le modalità di adesione al programma, in base alle quali le strutture territoriali, ai fini della presentazione della domanda di affiliazione, hanno l'obbligo di tenere un elenco cartaceo o informatico delle persone e dei nuclei familiari assistiti in maniera continuativa e di costituire, per ogni persona o nucleo familiare, un fascicolo che contenga documentazione anagrafica e sullo stato di indigenza (ad es., Isee, affidamento ai servizi sociali, disoccupazione, etc). È inoltre prevista la comunicazione dei dati relativi agli "assistiti continuativi", cioè degli indigenti "per i quali è stata effettuata una valutazione della condizione economica e sociale", nonché degli "assistiti saltuari", cioè di coloro che "vengono assistiti per far fronte a delle emergenze e per i quali l'erogazione avviene senza necessità di verificare la condizione individuale in maniera approfondita", la cui consistenza è stabilita in rapporto al numero totale

degli indigenti continuativi. Pertanto, il trattamento di dati personali dei beneficiari finali è previsto soltanto per gli "assistiti in via continuativa", il cui elenco nominativo deve essere trasmesso all'ente capofila, mentre i fascicoli personali devono essere conservati ed esibiti dalla struttura territoriale solo in fase di convenzionamento o di successive verifiche. Tali controlli, da parte dell'ente capofila, dell'Agea o di suoi delegati, sono previsti dalla normativa comunitaria per verificare la conformità della gestione alle finalità dell'aiuto come stabilito dalle norme del reg. (UE) 223/2014, relativo al Fondo di aiuti europei agli indigenti (v. Titolo V, Gestione e controllo). Con riferimento alla tipologia di dati personali che possono essere trattati dall'Agea, l'Ufficio ha chiarito che la documentazione richiesta agli assistiti continuativi non deve contenere informazioni di natura sensibile, in quanto strettamente finalizzata a comprovare la situazione di disagio economico, come previsto anche dal "Regolamento sul trattamento dei dati sensibili e giudiziari" adottato dall'Agea sul quale il Garante ha espresso il previsto parere (cfr. provv. 18 maggio 2006, doc. web n. 1299152). È stato, inoltre, chiarito che gli enti capofila e gli enti territoriali affiliati, possono trattare i dati personali dei propri aderenti ed assistiti, nel rispetto del quadro normativo di settore, in conformità all'informativa resa agli interessati (artt. 13, 23, 24 e 26 del Codice, autorizzazione generale n. 3 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, 11 dicembre 2014, n. 585, doc. web n. 3620014) (nota 20 luglio 2015).

Il Garante, con provvedimento 5 febbraio 2015 (n. 62, doc. web n. 3769046), ha espresso parere favorevole sullo schema di decreto direttoriale dell'Inps recante il disciplinare tecnico contenente le regole tecniche di sicurezza per la trasmissione e l'accesso alle informazioni del Sistema informativo Isee-(SII), di cui all'art. 12, comma 2, d.P.C.M. 5 dicembre 2013, n. 159, "Regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'Indicatore della situazione economica equivalente", sul quale il Garante ha fornito il parere di competenza con provvedimento 22 novembre 2012 (n. 361, doc. web n. 2174496). Lo schema di decreto è risultato conforme alle indicazioni fornite dall'Ufficio ai competenti uffici dell'Istituto nel corso di numerosi contatti, anche informali, volti a garantire il rispetto della disciplina in materia di protezione dei dati personali nell'ambito delle operazioni di raccolta e successivi trattamenti dei dati personali effettuati attraverso il SII e necessari al calcolo dell'Isee. Le principali indicazioni hanno riguardato le modalità di trattamento e le misure di sicurezza poste a garanzia dei dati trattati, nell'ambito delle quali è stato previsto, in particolare, che i flussi di dati per l'alimentazione del SII, tramite applicazioni web, avvenga su rete pubblica con l'utilizzo del protocollo SSL per garantire il trasporto cifrato delle informazioni. Nelle ipotesi in cui i flussi di dati vengono effettuati tramite cooperazione applicativa, invece, è stato previsto che si faccia riferimento al modello *advanced* di porta di dominio definito negli *standard* SPC di cooperazione applicativa e che la verifica degli accessi avvenga sulla base della mutua autenticazione fra i *server* dell'Istituto e quelli degli enti coinvolti. Sono stati ribaditi, inoltre, i princìpi di pertinenza, non eccedenza ed indispensabilità dei dati rispetto alle finalità perseguite, anche in riferimento alla consultazione delle informazioni autodichiarate da parte dell'ente erogatore per finalità di controllo e, a garanzia del rispetto di tali princìpi, sono stati previsti specifici controlli a campione da parte dell'Istituto (art. 11, commi 6 e 10, d.P.C.M. 5 dicembre 2013, n. 159; art. 11, comma 2, del Codice). Sono state individuate specifiche tecniche di anonimizzazione e aggregazione dei dati ai quali gli enti erogatori possono accedere a fini di programmazione dei singoli interventi nonché dei dari che devono essere trasmessi

al Ministero del lavoro e delle politiche sociali e, in caso di specifica richiesta, alle regioni e alle province autonome, per effettuare elaborazioni a fini di programmazione, di ricerca e di studio (art. 11, commi 4, 10, e 12, d.P.C.M. 5 dicembre 2013, n. 159). Particolare attenzione è stata posta sulle modalità di realizzazione dei controlli che la Guardia di finanza effettua sulla posizione reddituale e patrimoniale dei nuclei familiari dei soggetti beneficiari di prestazioni (art. 11, commi 11 e 13, d.P.C.M. 5 dicembre 2013, n. 159; 4, comma 2, d.m. 8 marzo 2013). Al riguardo, lo schema di decreto direttoriale esaminato evidenzia che gli accessi della Guardia di finanza avvengono in modalità web ovvero tramite cooperazione applicativa. Dal punto di vista funzionale, tali accessi si differenziano in due categorie: quelli effettuati nell'ambito di indagini specifiche e quelli effettuali nell'ambito della programmazione dell'attività di accertamento. Nel primo caso la Guardia di finanza può avere accesso all'attestazione riportante l'Isee, al contenuto della dsu, nonché agli elementi informativi necessari al calcolo, acquisiti dagli archivi amministrativi dell'Inps e dell'Agenzia delle entrate; nel secondo, il controllo della posizione reddituale e patrimoniale dei nuclei familiari dei soggetti beneficiari di prestazioni deve avvenire secondo criteri selettivi da definire, previo parere del Garante, in attuazione del protocollo di intesa adottato al fine di disciplinare le regole generali della reciproca collaborazione tra Inps e Guardia di finanza. L'Inps ha previsto che i caf e i comuni possano ricevere per gli interessati l'attestazione Isee, le dsu nonché gli elementi informativi necessari al calcolo dell'Isee. A tal fine, come indicato in fase istruttoria, i predetti soggetti devono inviare all'Istituto medesimo copia del mandato di assistenza, corredato dal documento di riconoscimento dell'interessato.

Al fine di impedire la creazione di autonome banche dati delle dsu presso i soggetti legittimati alla ricezione della stessa, l'Istituto ha predisposto una specifica funzione di *audit* e notifica sulla frequenza e numerosità delle posizioni interrogate nonché la registrazione dell'identificativo dell'operatore dell'ente che effettua l'accesso e del codice della posizione acceduta (artt. 10, comma 6, e 11, comma 4, d.P.C.M. 5 dicembre 2013, n. 159).

Il Garante, con provvedimento 2 aprile 2015 (n. 195, doc. web n. 3843693), ha espresso parere favorevole sullo schema di decreto direttoriale dell'Inps inerente le modalità attuative dei flussi informativi e disciplinare tecnico per la sicurezza della banca dati delle prestazioni sociali agevolate istituita presso l'Inps con decreto interministeriale dell'8 marzo 2013 al fine di rafforzare i controlli connessi all'erogazione di prestazioni sociali agevolate condizionate all'Isee (sul quale il Garante aveva fornito il parere di competenza con provv. 17 gennaio 2013, n. 14, doc. web n. 2300596) (artt. 2, comma 5, e 5 comma 5, d.m. 8 marzo 2013). La predetta banca dati è alimentata dagli enti locali e da ogni altro ente erogatore di prestazioni sociali agevolate, con le informazioni sulle prestazioni sociali agevolate, condizionate all'Isee, e sui soggetti che ne hanno beneficiato (art. 2, commi 1, 2 e 3, d.m. 8 marzo 2013). Ad essa accedono l'Inps, l'Agenzia delle entrate e la Guardia di finanza per lo svolgimento di attività di controllo (art. 4, commi 1 e 2, d.m. cit.). Le informazioni contenute nella banca dati sono poi trasmesse a diversi soggetti pubblici in forma anonima e aggregata per finalità di programmazione e monitoraggio nonché per elaborazioni a fini statistici, di ricerca e di studio (art. 4, commi 4, 5 e 6). Sulla base delle indicazioni fornite dall'Ufficio, l'Inps ha, in primo luogo, previsto che le convenzioni bilaterali per la definizione delle modalità tecniche e delle misure di sicurezza per l'accesso ai dati della banca dati prestazioni sociali agevolate da parte dell'Agenzia delle entrate e della Guardia di finanza debbano essere preventivamente sottoposte al Garante per le valutazioni di competenza. In secondo luogo, partico-