Anche in presenza di un obbligo di pubblicazione *online* le pp.aa. devono comunque selezionare i dati personali da inserire negli atti e documenti oggetto di pubblicazione e verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni nel rispetto del principio di pertinenza e non eccedenza dei dati personali nonché, nel caso dei dati sensibili, di indispensabilità.

Restano fermi alcuni divieti di diffusione di dati personali. In particolare, è sempre vietato diffondere dati idonei a rivelare lo stato di salute – ossia qualsiasi informazione da cui si possa desumere, anche indirettamente, 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 – nonché dati idonei a rivelare la vita sessuale quando la pubblicazione è effettuata per finalità di trasparenza (art. 4, comma 6, d.lgs. n. 33/2013).

L'indicizzazione dei dati nei motori di ricerca generalisti (ad es., Google) durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza. Vanno quindi esclusi gli altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (ad es., pubblicità legale sull'albo pretorio, pubblicazioni matrimoniali, ecc.).

Il Garante ha inoltre precisato che in ogni caso i dati pubblicati *online* non sono liberamente riutilizzabili da chiunque per qualunque finalità, poiché l'obbligo previsto dalla normativa in materia di trasparenza *online* della p.a. di pubblicare dati in "formato aperto" non comporta che tali dati siano anche "dati aperti", cioè liberamente utilizzabili da chiunque per qualunque scopo. Al fine di chiarire tale circostanza, le amministrazioni sono invitate a inserire nella sezione denominata "Amministrazione trasparente" dei propri siti web un *alert* con cui si informa il pubblico che i dati personali sono "riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva 2003/98/CE e d.lgs. n. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali".

È stato oltresì precisato che il periodo di mantenimento di dati, informazioni e documenti sul web coincide in linea di massima con il termine di cinque anni, ma anche che laddove atti, documenti e informazioni oggetto di pubblicazione obbligatoria per finalità di trasparenza contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

Nel caso di pubblicazione di atti e documenti, per finalità diverse da quelle di trasparenza, rimangono invece ferme le specifiche disposizioni di settore (ad es., quindici giorni per la pubblicazione delle deliberazioni all'albo pretorio degli enti locali ai sensi dell'art. 124, d.lgs. 18 agosto 2000, n. 267). Se, invece, la disciplina di settore non stabilisce un limite temporale alla pubblicazione degli atti, vanno individuati – a cura delle amministrazioni titolari del trattamento – congrui periodi di tempo entro i quali mantenerli *online*, ma questo lasso di tempo non può essere superiore al periodo ritenuto, caso per caso, necessario al raggiungimento degli scopi per i quali i dati personali stessi sono resi pubblici.

Anche alla luce di tali indicazioni il Garante è intervenuto in numerose questioni sottoposte alla propria attenzione di cui si riportano le più rilevanti.

Con riferimento alla diffusione di dati personali *online* in assenza di idonei presupposti normativi, è stata riscontrata una condotta non conforme alla disciplina applicabile in ordine ai dati personali contenuti in numerosi documenti pubblicati sui siti web istituzionali come, fra gli altri, i verbali della commissione elettorale comunale relativi alla revisione e all'aggiornamento dell'albo unico degli scrutatori

di seggio elettorale (con indicazione dei nominativi degli interessati, luogo e data di nascita, indirizzo, motivo della non inclusione o della cancellazione nell'albo degli scrutatori oppure notizia della relativa iscrizione) (nota 22 agosto 2014); i provvedimenti amministrativi di cancellazione anagrafica per irreperibilità (nota 4 dicembre 2014); le fotocopie di carte di identità o di patenti di guida (nota 8 gennaio 2014); i nomi degli utenti morosi che utilizzano il servizio *pre* e *post* scuola con indicazione del nome del bambino, quello del genitore, numero di cellulare, indirizzo dell'abitazione, scuola frequentata dal minore e la somma ancora non pagata per il servizio (nota 4 dicembre 2014); la copia degli atti da notificare e contestazioni di sanzioni amministrative (con indicazione in chiaro dei dati personali del destinatario del provvedimento) (nota 29 settembre 2014); le immagini in chiaro dei bambini in costume da bagno ammessi alla colonia estiva del comune (nota 19 agosto 2014); le deliberazioni pubblicate sull'albo pretorio degli enti locali per più di quindici giorni (nota 8 ottobre 2014).

Dati sanitari

Con riferimento alla diffusione di dati personali *online* idonei a rivelare lo stato di salute, il Garante è intervenuto nei confronti di un'azienda sanitaria che ha pubblicato in internet le delibere relative alla liquidazione di fatture per l'inserimento di un minore in una comunità terapeutica riabilitativa. A tali delibere erano state allegate le copie integrali delle fatture relative alla retta della comunità che contenevano in chiaro e per esteso i dati anagrafici del giovane (nome, cognome, data e luogo di nascita) causando una diffusione di dati sul suo stato di salute vietata dalle norme in materia di protezione dei dati personali (provv. 6 novembre 2014, n. 494, non pubblicato ai sensi dell'art. 24 del Regolamento del Garante del 1° agosto 2013). Sullo stesso tema, è stata riscontrata una condotta non conforme alla disciplina applicabile in ordine alla pubblicazione sul sito web istituzionale di determinazioni aventi a oggetto "il ricovero urgente in ospedale di persona affetta da malattia mentale" (Tso) con indicazione in chiaro dei dati dell'interessato e della relativa patologia (nota 22 agosto 2014), oppure la concessione dei benefici di cui all'art. 33, comma 3, l. n. 104/92 con espliciti riferimenti alla condizione di handicap della figlia di un dipendente avente diritto al predetto beneficio (nota 22 agosto 2014).

Dati giudiziari

È stata altresì stigmatizzata la pubblicazione sul sito web istituzionale di un comune del decreto del Ministro dell'interno di rigetto della domanda di cittadinanza contenente dati personali anche giudiziari dell'interessato (nota 14 gennaio 2014) ed è stato chiarito, a un comune che aveva intenzione di pubblicare sul sito internet istituzionale il certificato del casellario giudiziale del sindaco, degli assessori e dei membri di "maggioranza" dei componenti il consiglio comunale, che il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21, comma 1) (nota 22 agosto 2014).

Sempre in tema di trasparenza, il Garante è stato poi interpellato con riferimento alla questione della reperibilità in rete, tramite i motori di ricerca generalisti (es. Google), di dati personali anche sensibili e giudiziari contenuti negli atti pubblicati sul sito web istituzionale della Camera dei deputati, nonché sul profilo della conoscibilità dei documenti formati e acquisiti dalle Commissioni parlamentari di inchiesta.

In ordine alla prima questione, confermando i precedenti orientamenti in materia (cfr. Relazione 2012, p. 70), è stato fatto presente che i lavori delle istituzioni parlamentari sono soggetti a regime di pubblicità (artt. 65 e 144 del regolamento della Camera e 33 del regolamento del Senato) e che i principi inerenti al trattamento dei dati sensibili e giudiziari sono applicabili ai trattamenti svolti dalla Presidenza della

Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte Costituzionale "in conformità ai rispettivi ordinamenti" (art. 22, comma 12, del Codice). È stato altresì ricordato che l'Ufficio di Presidenza della Camera dei deputati, con la delibera n. 46 del 2013, come modificata dalla delibera n. 53 del 2013, ha adottato una disciplina concernente la "Procedura in ordine a richieste concernenti dati personali contenuti in atti parlamentari" (disponibile in *www.camera.it/leg17/672?conoscerelacamera=316*) relativa alle modalità con cui i cittadini possono fare istanza direttamente alla Presidenza della Camera dei deputati con riferimento "a loro dati personali contenuti in atti parlamentari pubblicati sul sito internet della Camera dei deputati" (nota 5 giugno 2014).

In relazione, invece, alla pubblicazione sul sito istituzionale di atti e documenti delle Commissioni parlamentari d'inchiesta è stato rappresentato che esistono due diverse tipologie di atti e documenti: quelli "formati" dalla Commissione d'inchiesta stessa (come i resoconti delle audizioni) e quelli, invece, solo "acquisiti" dalla Commissione stessa in quanto prodotti da soggetti esterni.

Fino a oggi, tale tipologia di atti e documenti formati o acquisiti dalle Commissioni parlamentati d'inchiesta è stata soggetta a un preciso regime di pubblicità, differenziato in ragione della "diversa natura dei documenti in esame", che prevede la pubblicazione sul sito web istituzionale della Camera degli atti formati dalle Commissioni, in quanto soggetti al principio di pubblicità dei lavori parlamentari ai sensi dell'art. 64 Cost., e la mera consultabilità, presso i locali dell'archivio storico dei documenti acquisiti dalla Commissione nel corso dell'inchiesta da parte di chiunque ne faccia richiesta.

Con riferimento all'interesse alla conoscibilità dei documenti "acquisiti" dalle Commissioni d'inchiesta, occorre tenere conto che gli stessi sono stati oggetto del vaglio della Commissione e le informazioni ritenute di interesse ai fini dell'inchiesta sono state presumibilmente evidenziate nelle relazioni – di maggioranza ed, eventualmente, di minoranza – già integralmente pubblicate. Di conseguenza, le eventuali ulteriori informazioni che emergano dai documenti esterni acquisiti dalla Commissione – e che giustifichino la successiva ostensione dei documenti medesimi – potrebbero essere state ritenute dai diversi componenti della Commissione irrilevanti o addirittura inattendibili.

Considerata quindi la notevole varietà del contenuto e dei dati personali, anche sensibili e giudiziari, inseriti soprattutto negli atti esterni acquisiti dalle Commissioni parlamentari d'inchiesta per l'esercizio delle proprie funzioni, spetta ai competenti organi della Camera – alla luce dei principi in materia di protezione dei dati personali prima richiamati – effettuare il più corretto bilanciamento fra l'interesse alla piena conoscibilità della documentazione dell'attività delle menzionate Commissioni e la riservatezza delle informazioni in essa contenute.

In ogni caso, tenendo conto della "diversa natura dei documenti in esame", l'Ufficio ha ritenuto che gli organi della Camera hanno correttamente differenziato il relativo regime di pubblicità, prevedendo per gli atti formati dalla Commissione d'inchiesta la "pubblicazione" (art. 4, comma 1, lett. *m*), del Codice) su internet e per gli altri documenti la sola "comunicazione" degli stessi (art. 4, comma 1, lett. *l*), del Codice), nella forma della consultabilità a richiesta dei soggetti eventualmente interessati, assicurando in tal modo il pubblico interesse alla piena conoscibilità degli atti esterni acquisiti dalle Commissioni.

In tale cornice, è stato ritenuto che, per favorire una maggiore facilità di accesso agli atti esterni acquisiti dalle Commissioni parlamentari d'inchiesta, nel pieno rispetto dell'interesse alla loro massima conoscibilità, trattando le Commissioni d'inchiesta di questioni di "pubblico interesse", possono essere comunque predisposte

modalità di accesso *online* alle medesime informazioni, tramite accessi selettivi, ai soli soggetti che ne facciano richiesta appositamente identificati. Tale soluzione, che è stata rappresentata come un'opzione praticabile, deve ritenersi preferibile rispetto alla diffusione in quanto assicura un corretto bilanciamento tra le esigenze di semplificazione delle modalità di accesso a informazioni di "pubblico interesse" e il diritto alla protezione dei dati personali.

Al riguardo, per completezza è stato ricordato che il Cad, per consentire l'accesso ai servizi erogati in rete da parte delle pp.aa, prevede l'utilizzo della carta d'identità elettronica e della carta nazionale dei servizi, oppure di strumenti diversi purché idonei a consentire "l'individuazione del soggetto che richiede il servizio" (art. 64, commi 1 e 2, d.lgs. 7 marzo 2005, n. 82) (nota 19 giugno 2014).

4.5. *La documentazione anagrafica e la materia elettorale*

Per quanto riguarda la materia elettorale, il Garante ha adottato un nuovo provvedimento generale in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale (provv. 6 marzo 2014, n. 107, doc. web n. 3013267) che introduce notevoli profili di semplificazione per il trattamento dei dati personali.

Con il citato provvedimento viene introdotto uno specifico regime di esonero dall'obbligo di rendere l'informativa per partiti, movimenti politici, sostenitori e singoli candidati nel caso in cui si utilizzino dati personali estratti da particolari registri ed elenchi pubblici (ad es., liste elettorali ed assimilate). Le prescrizioni in materia di esonero, infatti, non hanno più, come in passato, vigenza provvisoria e circoscritta a determinate consultazioni (cfr. provv.ti 12 febbraio 2004, n. 45, doc. web n. 634369; 7 settembre 2005, n. 212, doc. web n. 1165613; 24 aprile 2013, n. 228, doc. web n. 2404305), ma sono applicabili ogni qual volta si svolgano consultazioni politiche, amministrative o referendarie, o iniziative per selezione di candidati (cd. primarie), nel rispetto di presupposti, condizioni e limiti, anche temporali, individuati con il predetto provvedimento. L'Autorità ha così inteso evitare che, nel breve arco temporale in cui si svolgono le consultazioni (politiche, amministrative o referendarie), un alto numero di interessati riceva un elevato numero di informative analoghe riguardanti il trattamento dei dati personali da parte di più soggetti impegnati in iniziative di comunicazione politica. Ciò in considerazione del fatto che i messaggi elettorali vengono generalmente inviati per posta all'indirizzo risultante dalle liste elettorali che, per una precisa scelta normativa, costituiscono la fonte privilegiata di dati personali lecitamente utilizzabili per i predetti fini (art. 51, d.P.R. 20 marzo 1967, n. 223, come modificato dall'art. 177, comma 5, del Codice).

Per ciò che concerne le modalità di utilizzo di dati personali estratti da fonti pubbliche – vale a dire le informazioni contenute in registri, elenchi, atti o documenti detenuti da un soggetto pubblico e al tempo stesso accessibili in base ad un'espressa disposizione di legge o di regolamento – viene ribadito che non è necessario richiedere il consenso degli interessati, ma occorre rispettare i limiti e le modalità eventualmente stabilite dall'ordinamento per accedere a tali fonti (ad es., se è richiesta l'identificazione di chi ne chiede copia o se l'accesso è consentito solo in determinati periodi o per determinate finalità) o per utilizzarle (ad es., obbligo di indicare la fonte dei dati o di rispettare le finalità che la legge stabilisce per determinati elenchi). Possono, pertanto, essere utilizzate le liste elettorali detenute presso i comuni (art. 51, d.P.R. 20 marzo 1967, n. 223, come modificato dall'art. 177, comma 5, del Codice), l'elenco degli elettori italiani che votano all'estero per

le elezioni del Parlamento europeo (art. 4, d.l. 24 giugno 1994, n. 408, convertito con l. 3 agosto 1994, n. 483), le liste aggiunte dei cittadini elettori di uno Stato membro dell'Unione europea residenti in Italia e che intendano ivi esercitare il diritto di voto alle elezioni del Parlamento europeo (artt. 1 e ss., d.lgs. 12 aprile 1996, n. 197), l'elenco provvisorio dei cittadini italiani residenti all'estero aventi diritto al voto (art. 5, comma 8, d.P.R. 2 aprile 2003, n. 104; per i Comitati degli italiani all'estero, art. 13, comma 2, l. 23 ottobre 2003, n. 286; art. 11, comma 2, d.P.R. n. 395/2003).

Anche alla luce delle segnalazioni pervenute nel corso degli anni, il provvedimento individua alcune fonti documentali detenute dai soggetti pubblici che non possono essere utilizzate per finalità di propaganda elettorale. Tra queste sono ricomprese: le Anagrafi comunali della popolazione residente (artt. 33 e 34, d.P.R. 30 maggio 1989, n. 223; art. 62, d.lgs. 7 marzo 2005, n. 82; d.P.C.M. 23 agosto 2013, n. 109), e ciò anche se il richiedente è un amministratore locale o il titolare di una carica elettiva che intenda utilizzarle ai predetti fini o per intrattenere pubbliche relazioni di carattere personale; gli archivi dello stato civile (art. 450 c.c.; d.P.R. 3 novembre 2000, n. 396); gli schedari dei cittadini residenti nella circoscrizione presso ogni ufficio consolare (art. 8, d.lgs. 3 febbraio 2011, n. 71); i dati raccolti dai soggetti pubblici nello svolgimento delle proprie attività istituzionali o, in generale, per la prestazione di servizi, gli elenchi di iscritti ad albi e collegi professionali (art. 61, comma 2, del Codice); gli indirizzi di posta elettronica tratti dall'indice nazionale degli indirizzi Pec delle imprese e dei professionisti (d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, che ha inserito l'art. 6-*bis* nel d.lgs. 7 marzo 2005, n. 82).

Viene, inoltre, ribadito il divieto di utilizzare le liste elettorali di sezione già utilizzate nei seggi, sulle quali sono annotati i dati relativi ai non votanti e che sono utilizzabili solo per controllare la regolarità delle operazioni elettorali (art. 62, d.P.R. 16 maggio 1960, n. 570), nonché i dati annotati nei seggi da scrutatori e rappresentanti di lista per lo svolgimento delle operazioni elettorali. Tali dati, se conosciuti, devono essere trattati con la massima riservatezza nel rispetto del principio costituzionale della libertà e della segretezza del voto, avuto anche riguardo alla circostanza che la partecipazione o meno ai *referendum* o ai ballottaggi può evidenziare di per sé anche un eventuale orientamento politico dell'elettore.

Non possono, parimenti, essere utilizzati i dati personali resi disponibili sui siti istituzionali dei soggetti pubblici sulla base di obblighi derivanti dalle disposizioni in materia di trasparenza delle informazioni concernenti l'organizzazione e l'attività delle pp.aa. (l. 18 giugno 2009, n. 69; d.lgs. 14 marzo 2013, n. 33), nonché da altre norme di settore. Si pensi, ad esempio, agli atti contenenti dati personali pubblicati sull'albo pretorio *online*, alla pubblicità degli esiti concorsuali, agli atti di attribuzione a persone fisiche di vantaggi economici comunque denominati, agli organigrammi degli uffici pubblici recanti anche recapiti telefonici e indirizzi di posta elettronica dei dipendenti, alle informazioni riferite agli addetti ad una funzione pubblica. La circostanza che tali dati siano resi pubblicamente conoscibili *online* per finalità di trasparenza non consente che gli stessi siano liberamente riutilizzabili da chiunque e per qualsiasi scopo, ivi compreso, quindi, il perseguimento di finalità di propaganda elettorale e connessa comunicazione politica.

Anche i dati acquisiti dai titolari di alcune cariche elettive per l'esercizio del mandato e la partecipazione alla vita politico-amministrativa dell'ente (art. 43, comma 2, d.lgs. 18 agosto 2000, n. 267), ovvero da chi riveste cariche pubbliche non elettive o, più in generale, incarichi pubblici, per lo svolgimento dei propri compiti istituzionali, non possono essere utilizzati per le finalità in esame. Come detto, la fina-

lizzazione esclusiva dei dati così ottenuti all'esercizio del mandato o allo svolgimento dei compiti istituzionali previsti dalla legge, costituisce, al tempo stesso, il presupposto che legittima l'accesso e che ne limita la portata.

Infine, il provvedimento ribadisce il divieto di utilizzo di particolari indirizzari o dati raccolti da strutture sanitarie, pubbliche e private, ovvero da singoli professionisti sanitari, nell'ambito delle attività di diagnosi e cura da essi svolti, al fine di veicolare messaggi di comunicazione politica volti a sostenere la candidatura di personale medico o comunque legato alla struttura sanitaria presso la quale l'interessato si è recato per fini di cura.

Anagrafe nazionale della popolazione residente

Per quanto riguarda la fase attuativa della nuova Anagrafe nazionale della popolazione residente (Anpr), istituita dall'art. 62 del Cad (introdotto dall'art. 2, comma 1, d.l. n. 179/2012, convertito dalla l. n. 221/2012), l'Autorità ha fornito il proprio parere sui decreti che definiscono i tempi e le modalità per l'istituzione della suddetta banca dati presso il Ministero dell'interno. Come è noto, l'Anpr subentra all'Indice nazionale delle anagrafi (Ina) e all'Anagrafe degli italiani residenti all'estero (Aire) nonché alle singole banche dati anagrafiche attualmente tenute dai comuni italiani, determinando in tal modo la centralizzazione presso il Ministero dell'interno di un numero cospicuo di informazioni personali.

L'Anpr è preordinata ad assicurare ai comuni la disponibilità dei dati anagrafici della popolazione residente per lo svolgimento delle funzioni di anagrafe e di stato civile, nonché i servizi informativi necessari per lo svolgimento delle altre funzioni istituzionali. Allo stesso modo, le altre pubbliche amministrazioni dovranno avvalersi dell'Anpr per la raccolta delle informazioni anagrafiche necessarie allo svolgimento dei propri compiti istituzionali. Le informazioni anagrafiche, una volta rese dagli interessati, si intendono acquisite anche dalle altre amministrazioni, senza necessità di ulteriori adempimenti in capo ai singoli, garantendo l'allineamento con le altre banche dati.

In tale percorso attuativo il Garante ha fornito le proprie indicazioni in ordine alle garanzie e alle misure di sicurezza da adottare per la raccolta e il trattamento dei dati, alle modalità e ai tempi di conservazione, all'esattezza ed all'integrità dei dati ed all'allineamento, nella prima fase, con i dati contenuti nelle banche dati dei comuni, alle modalità di accesso ai servizi resi dall'Anpr da parte dei comuni stessi e delle altre pp.aa, ai criteri per l'interoperabilità con le altre banche dati di interesse nazionale secondo le regole del sistema pubblico di connettività (parere 17 aprile 2014, n. 202, doc. web n. 3105794; d.P.C.M. 10 novembre 2014, n. 194, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) e di definizione del piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente, in *G.U.* 8 gennaio 2015, n. 5).

Il Garante è stato inoltre chiamato ad esprimere il parere sullo schema di decreto del Presidente della Repubblica in tema di "adeguamento del regolamento anagrafico della popolazione residente approvato con d.P.R. 30 maggio 1989, n. 223, alla disciplina istitutiva dell'Anagrafe nazionale della popolazione residente" (provv. 22 gennaio 2015, n. 31, doc. web n. 3738655).

Ancora con riferimento alla materia anagrafica, la Prefettura di Avellino, ha formulato un quesito in merito alla possibilità per il Dipartimento di prevenzione dell'Asl di Avellino di acquisire elenchi e vari dati anagrafici relativi ai cittadini residenti nei comuni della provincia, finalizzati al funzionamento del Registro provinciale dei tumori della popolazione. Al riguardo, l'Asl ha precisato che i dati dei comuni che rientrano nell'area di riferimento del Registro tumori risulterebbero necessari per verificare la correttezza delle anagrafi sanitarie e per rilevare il dettaglio degli indirizzi dell'intera popolazione di riferimento, indispensabile per gli

studi di epidemiologia ambientale. L'Ufficio, dopo aver ricordato che la disciplina sugli atti anagrafici consente di rilasciare, anche periodicamente, elenchi di iscritti nell'anagrafe della popolazione residente "alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", e che è anche previsto il rilascio di "dati 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), ha precisato che la prima delle finalità esplicitate – verifica della "correttezza delle anagrafi sanitarie" presenti nel Registro – può essere effettuata anche avvalendosi delle modalità di comunicazione telematica previste dall'art. 58, comma 2, del Cad. Per quanto riguarda, invece, la richiesta del dettaglio degli indirizzi dell'intera popolazione di riferimento, indispensabile per gli studi di epidemiologia ambientale, è stato evidenziato che tale esigenza deve essere valutata alla luce delle specifiche disposizioni che prevedono "la raccolta, l'elaborazione e la registrazione di dati statistici completi [...] dei casi di tumore anche infantili che si verificano nella popolazione della Regione Campania", ovvero "dei dati individuali, sanitari ed amministrativi, sugli ammalati di tumore", e non dell'intera popolazione del territorio di competenza (cfr. art. 1, comma 2 lett. *a*) e art. 3, comma 1, l.r. 10 luglio 2012, n. 19, concernente l'istituzione del Registro tumori della popolazione della Regione Campania). Infine, dopo aver richiamato il quadro normativo di riferimento per i trattamenti per scopi statistici e scientifici (artt. 104 e ss. del Codice, All. A.4, codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, doc. web n. 1556635), è stato puntualizzato che l'acquisizione di dati ed altre informazioni anagrafiche relativi all'intera popolazione è consentita per lo svolgimento di specifici scopi scientifici – tra i quali rientrano anche gli studi epidemiologici – purché "chiaramente determinati" e specificamente indicati in relazione alla singola richiesta (art. 105 del Codice). Tali scopi devono, inoltre, essere resi noti agli interessati nei modi previsti dall'art. 13 del Codice ed il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto (art. 105, commi 2 e 4, del Codice) (nota 15 settembre 2014).

4.6. *L'istruzione scolastica ed universitaria*

Risultano sempre numerosi i chiarimenti richiesti in relazione al trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica ed universitaria.

Con riferimento ai dati pubblicati tramite gli albi scolastici, è stato segnalato al Garante che un istituto statale comprensivo ha affisso agli albi delle scuole ed alle bacheche esterne dei plessi il testo di una comunicazione elettronica, nell'ambito della quale risultava visibile l'indirizzo di posta elettronica privato di uno dei destinatari, docente presso l'istituto medesimo.

Al riguardo, è stato ribadito che i soggetti pubblici possono diffondere dati personali, diversi da quelli sensibili e giudiziari, unicamente quando tale specifica operazione di trattamento risulta ammessa da una norma di legge o di regolamento (art. 19, comma 3, del Codice). Ciò posto, l'Autorità, considerato che l'indirizzo di posta elettronica costituisce dato personale, ai sensi dell'art. 4, comma 1, lett. *b*), del Codice, e che la citata operazione di trattamento integra una diffusione di dati di dati personali, ai sensi dell'art. 4 comma 1, lett. *m*), del Codice, dopo aver constatato l'assenza di una base normativa che legittimasse la citata operazione di trattamento, ha

rilevato l'illiceità della predetta diffusione ed ha vietato all'istituto l'ulteriore diffusione, con qualunque mezzo, ivi compresa l'affissione all'albo ed alle bacheche delle scuole, del dato relativo all'indirizzo di posta elettronica personale del segnalante (provv. 23 gennaio 2014, n. 28, doc. web n. 2929890).

Un'altra segnalazione ha riguardato un istituto scolastico statale che, nel documento di programmazione di una classe, al capitolo programmazione alunni dislessici, aveva riportato i nominativi degli alunni affetti da disturbi specifici dell'apprendimento (dsa).

Al riguardo, l'Ufficio ha evidenziato che le istituzioni scolastiche pubbliche possono trattare dati sensibili, tra i quali rilevano quelli idonei rivelare lo stato di salute, solo se autorizzati da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui la legge, pur specificando la finalità di rilevante interesse pubblico, non evidenzi, altresì, i tipi di dati sensibili e giudiziari e di operazioni eseguibili, il trattamento è consentito, nel rispetto dei principi di cui all'art. 22 del Codice, ed, in particolare, del principio di indispensabilità, solo per lo svolgimento di specifiche finalità, in riferimento ai tipi di dati e di operazioni identificati e resi pubblici dal titolare in un atto di natura regolamentare adottato in conformità al parere espresso dal Garante (artt. 20 e 22 del Codice; l. 8 ottobre 2010, n. 170; d.m. 12 luglio 2011, n. 5669).

Su tali basi, l'Ufficio ha rilevato la non conformità della predetta condotta alla disciplina in materia di protezione dei dati personali, nella misura in cui non è risultato effettivamente indispensabile alle finalità perseguite l'indicazione dei nominativi degli studenti affetti da dsa nel citato documento. Anche in questo caso, tuttavia, l'Ufficio non ha promosso l'adozione di un provvedimento da parte del Collegio, tenuto conto del fatto che la condotta aveva esaurito i suoi effetti e delle rassicurazioni fornite dal titolare del trattamento circa l'immediato oscuramento dei predetti dati personali dal documento di programmazione della classe (nota 8 gennaio 2014).

È stato inoltre segnalato che una scuola superiore di secondo grado ha diffuso sul proprio sito internet istituzionale gli elenchi degli alunni, distinti per classe, per supposte finalità di trasparenza (art. 19, comma 3, del Codice).

A seguito della richiesta di chiarimenti avanzata dall'Ufficio, l'istituto scolastico ha provveduto all'immediata cancellazione dei predetti elenchi. Al riguardo, è stato, infatti evidenziato che tali dati non rientrano tra quelli oggetto di pubblicazione obbligatoria per finalità di trasparenza, ai sensi del d.lgs. n. 33/2013, ed è stato ribadito che la diffusione di dati personali da parte di soggetti pubblici è ammessa unicamente quando è prevista da una norma di legge o di regolamento, nel rispetto del principio di pertinenza e non eccedenza (art. 19, comma 3, e art. 11, comma 1, lett. *d*), del Codice) e che, quindi, le amministrazioni, prima di diffondere sui propri siti istituzionali atti e documenti contenenti dati personali, devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo di pubblicazione (punto 2, provv. 15 maggio 2014, n. 243, doc. web n. 3134436; nota 8 gennaio 2015).

Giudizi relativi ai partecipanti alla procedura di abilitazione scientifica nazionale

Nell'ambito dell'attività dell'Ufficio è emerso che il Ministero dell'istruzione, dell'università e della ricerca ha diffuso sul proprio sito internet istituzionale gli atti e i giudizi individuali, anche negativi, relativi ai singoli partecipanti alla procedura di abilitazione scientifica nazionale per l'accesso al ruolo dei professori universitari, a norma dell'art. 16, l. 30 dicembre 2010, n. 240, consentendone, altresì, la reperibilità anche attraverso i più comuni motori di ricerca generalisti (quali Google).

Come detto, il Codice dispone che i soggetti pubblici, nell'ambito delle proprie competenze istituzionali, possono diffondere dati personali solo qualora tale operazione di trattamento sia ammessa da una norma di legge o di regolamento. La dif-

fusione, nel rispetto dei principi di necessità e proporzionalità, può durare solo per il tempo necessario allo scopo per il quale è stata effettuata (artt. 3, 11, 18 e 19, comma 3, del Codice).

Con riferimento alla diffusione dei giudizi, anche negativi, sui singoli candidati, è emerso che tale specifica operazione di trattamento è espressamente prevista, per un periodo di 120 giorni, dall'art. 16, l. n. 240/2010 e dall'art. 8, comma 9, d.P.R. n. 222/2011 (Regolamento concernente il conferimento dell'abilitazione scientifica nazionale per l'accesso al ruolo dei professori universitari, a norma dell'art. 16, l. 30 dicembre 2010, n. 240). La circostanza che tale diffusione possa, legittimamente, concernere anche i giudizi negativi dei singoli candidati è stata altresì motivata alla luce dei pareri forniti dal Consiglio di Stato in sede consultiva sul predetto regolamento, in base ai quali tali procedure, consentendo l'accesso a ruoli di estremo valore culturale, devono essere improntate alla massima trasparenza per consentire il controllo diffuso dell'intera comunità scientifica.

Con riferimento, invece, alla reperibilità anche attraverso i più comuni motori di ricerca generalisti, dei giudizi individuali dei candidati, accertato che tale possibilità risulta sproporzionata rispetto alle finalità del trattamento, a seguito dell'intervento dell'Autorità ed al fine di garantire un elevato *standard* di tutela del diritto alla protezione dei dati personali nell'ambito del trattamento in esame, il Ministero ha assicurato la rimozione dell'indicizzazione della pagine riportanti i risultati dell'abilitazione scientifica nazionale e l'implementazione di idonee misure atte ad impedire nuove indicizzazioni simili (nota 1° luglio 2014).

Archivio "Andrea Devoto"

Un interessante caso ha riguardato l'Università degli Studi di Firenze che ha in concessione il noto Archivio "Andrea Devoto", di proprietà della Regione Toscana, contenente le interviste che negli anni 80 il neuropsichiatra e psicologo Andrea Devoto rivolse, nell'ambito di uno studio, ad alcuni deportati sopravvissuti ai campi di sterminio nazisti. Da tali interviste emergono ovviamente dati sensibili, idonei a rivelare lo stato di salute degli intervistati dopo la deportazione.

Ciò posto, l'Ateneo ha formulato un quesito circa la possibilità di rendere consultabili i materiali contenuti nell'Archivio Devoto ed eventualmente consentire la pubblicazione delle interviste, procedendo alla cancellazione dei nominativi degli interessati.

Al riguardo, l'Ufficio ha evidenziato che il Codice in materia di protezione dei dati personali rinvia al codice dei beni culturali e del paesaggio (d.lgs. 22 gennaio 2004, n. 42) per l'individuazione della disciplina relativa alla consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati (art. 103 del Codice; art. 122, comma 1, lett. *b*) e 126, comma 3, del codice dei beni culturali e del paesaggio, cit.). Inoltre, in base al codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, All. A.2 al Codice (adottato ai sensi dell'art. 102 del Codice) – la cui osservanza costituisce condizione essenziale per la liceità dei trattamenti di dati personali per la predetta finalità – l'accesso agli archivi pubblici è libero, con eccezione dei documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data, e quelli contenenti i dati personali, sensibili e giudiziari, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale oppure rapporti riservati di tipo familiare (art. 10, commi 1 e 2, codice di deontologia; art. 122, comma 1, lett. *b*), del codice dei beni culturali e del paesaggio, cit.).

Con riferimento, invece, alla possibilità che le interviste dei pazienti vengano diffuse adottando accorgimenti idonei a rendere non identificabili gli intervistati, ad es. cancellando i nominativi degli stessi, è stato evidenziato che la semplice cancel-

lazione degli identificativi diretti non è una tecnica idonea a garantire (con certezza) l'anonimizzazione dei dati personali. Infatti, fintantoché persistano elementi sufficienti per consentire l'identificazione della persona interessata, le informazioni trattate devono considerarsi dati personali, ancorché indirettamente identificativi, e come tali soggetti alla specifica disciplina di settore sopra richiamata (artt. 4, comma 1, lett. *b*) e *n*), del Codice).

È stato, altresì, evidenziato che il Ministro dell'interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'interno, può rilasciare l'autorizzazione alla consultazione dei documenti riservati prima dei termini sopra indicati agli utenti che presentino uno specifico progetto di ricerca. Tale autorizzazione, che è personale e non delegabile a soggetti terzi, può contenere specifiche cautele volte a tutelare i diritti, la libertà e la dignità delle persone interessate (art. 10, del menzionato codice di deontologia; artt. 123 e 126, comma 3, del codice dei beni culturali e del paesaggio). L'Ufficio ha ricordato, infine, che gli archivisti possono trattare i documenti conservati negli archivi contenenti dati personali, in conformità alle regole generali di condotta individuate nel citato codice di deontologia volte, in particolare, a favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati (nota 17 settembre 2014).

4.7. *L'attività fiscale e tributaria*

È stato definito un reclamo concernente un trattamento di dati personali effettuato dall'Agenzia delle entrate di Latina nell'ambito di un accertamento tributario. Ritenuto il prezzo dichiarato in atti non congruo in relazione alle quotazioni della banca dati dell'Osservatorio del mercato immobiliare (Omi), l'Agenzia notificava ad un soggetto terzo un avviso di rettifica e liquidazione, che riportava in motivazione informazioni personali relative alla reclamante (ed in particolare che la stessa, dante causa dell'immobile in questione, non si era presentata a fornire dati e notizie relativamente ai rapporti finanziari, al fine di giustificare l'ammontare del saldo passivo di tali movimentazioni). L'istruttoria ha evidenziato che le indagini bancarie effettuate dalla menzionata Agenzia erano necessarie per acquisire elementi probatori utili a ricostruire il corrispettivo dichiarato nell'atto di cessione del fabbricato, che rilevava uno scostamento superiore al 50% alle rilevazioni della banca dati Omi e che la motivazione dell'avviso di liquidazione, di conseguenza, doveva evidenziare le informazioni reperite a seguito delle predette indagini finanziarie al fine di sostenere la pretesa tributaria. Tanto premesso, l'Ufficio ha ritenuto leciti e conformi ai principi di pertinenza e non eccedenza, i trattamenti di dati personali effettuati dall'Agenzia delle entrate. Con riferimento alla tipologia dei dati personali riportati nella motivazione dell'atto, la normativa di settore prevede, infatti, che l'avviso di rettifica e di liquidazione della maggiore imposta "deve indicare i presupposti di fatto e le ragioni giuridiche che lo hanno determinato" e che "l'accertamento è nullo se non sono osservate le disposizioni di cui al presente comma" (art. 52, comma 2, d.P.R. n. 131/1986). Infine, data la natura solidale dell'obbligazione tributaria in questione (art. 57, d.P.R. n. 131/1986, per l'imposta di registro; art. 11, d.lgs. n. 347/1990, per l'imposta ipotecaria e catastale), l'atto di accertamento dell'amministrazione finanziaria poteva essere notificato a ciascuno dei coobbligati, tutti legittimati a conoscerne il contenuto; di conseguenza, è stata ritenuta lecita la comunicazione dei dati della reclamante ai predetti (nota 17 ottobre 2014).

Il Garante, su richiesta del Consiglio di Stato, ha fornito al Ministero dell'economia e delle finanze un parere sul nuovo schema di Contratto di servizi quadro 2012-2017, regolante il rapporto per la gestione *in house* del sistema informativo della fiscalità tra l'Amministrazione finanziaria nel suo complesso e la Sogei S.p.A., quale suo ente strumentale preposto al settore dell'*Information and Communication Technology*.

Al riguardo, il Garante, vista l'estrema delicatezza dei dati personali trattati nell'ambito del sistema informativo della fiscalità, nonché il rilevante valore economico dell'affidamento, ha fornito al Ministero alcune indicazioni relative alle previsioni contrattuali in modo da assicurare all'amministrazione un maggior livello di prestazione relativamente ai servizi aventi un diretto impatto sulla sicurezza e sulla protezione dei dati personali, quali la protezione perimetrale, il rilevamento di intrusioni e il "*disaster recovery*". Sono state inoltre fornite indicazioni riguardo ai trattamenti di dati personali che possono avere luogo a seguito dell'adozione di strumenti di filtraggio della c.d. navigazione web (provv. 13 febbraio 2014, n. 68 doc. web n. 3001879).

4.8. *La videosorveglianza in ambito pubblico*

Come già avvenuto negli ultimi anni l'Autorità è stata più volte chiamata a esprimersi in ordine al trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico. In particolare, nel dare riscontro ad un comune, l'Ufficio ha fornito i necessari chiarimenti sulla durata della conservazione delle immagini registrate, facendo presente che per i comuni, e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, fatte salve speciali esigenze di ulteriore conservazione (cfr. punto 3.4, provv. 8 aprile 2010, doc. web n. 1712680; art. 6, comma 8, d.l. 23 febbraio 2009, n. 11 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 23 aprile 2009, n. 38) (nota 25 marzo 2014).

Ove si intenda, invece, conservare le immagini registrate per un periodo superiore alla settimana, l'Ufficio ha ricordato ad un istituto scolastico che una richiesta in tal senso deve essere sottoposta ad una verifica preliminare dell'Autorità, ai sensi dell'art. 17 del Codice, e che la congruità di un termine più ampio di conservazione va adeguatamente motivata facendo riferimento ad una specifica esigenza di sicurezza, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità (cfr. punto 3.4. del citato provvedimento generale) (nota 19 dicembre 2014).

Sempre con riferimento alla durata della conservazione delle immagini registrate, un centro di ricerca privato aveva richiesto, attraverso la verifica preliminare del Garante (art. 17 del Codice), di poter allungare i tempi di conservazione delle immagini registrate presso le aree interne del centro per un periodo di trenta anni, in corrispondenza alla durata di un progetto di ricerca effettuato dallo stesso. Considerata la peculiarità dell'istanza, sono stati chiesti chiarimenti, anche in occasione di un incontro tenutosi presso la sede dell'Ufficio, volti a conoscere se, nell'ambito dell'attività di monitoraggio del processo lavorativo relativo al progetto di ricerca, le telecamere rilevassero o meno immagini dei lavoratori in modo da renderli identificabili. Alla luce delle indicazioni fornite durante il citato incontro, il centro di ricerca ha sospeso la richiesta di verifica preliminare riservandosi di presentare una nuova richiesta, formulata all'esito delle necessarie valutazioni (note 5 giugno e 24 dicembre 2014).

Diversi sono stati poi gli aspetti presi in considerazione nel fornire indicazioni ad alcuni comuni che avevano attivato sistemi di videosorveglianza nell'ambito delle attività di controllo amministrative.

In un caso (cfr. nota 25 marzo 2014) è stato rilevato che l'utilizzo di sistemi di videosorveglianza risulta lecito per accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente, solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi (art. 13, l. 24 novembre 1981, n. 689).

È stata altresì esaminata una segnalazione con la quale si lamentava la comunicazione da parte di un comune ad un'emittente televisiva di alcuni dati personali contenuti nelle immagini riprese da sistemi di videosorveglianza comunale relative a cittadini che conferivano in modo non conforme i rifiuti. Il comune, interpellato dall'Ufficio, ha chiarito che i cittadini ripresi non erano riconoscibili, in quanto non ne venivano mostrati chiaramente i volti; né poteva desumersi la residenza dei presunti trasgressori soltanto dalle immagini relative alla via della città ove le telecamere erano installate. Pertanto, l'Ufficio non ha ravvisato gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (nota 19 gennaio 2015).

In un altro caso, sempre nell'ambito dell'attività di controllo comunale, è stata avviata un'istruttoria nei confronti di un comune di rilevanti dimensioni, il cui corpo di polizia locale aveva attivato un *account* su *Twitter* al fine di ricevere segnalazioni da parte dei cittadini in ordine a problematiche legate alla cd. "sosta selvaggia" e a situazioni di degrado o di insicurezza urbana. Dall'istruttoria preliminare era risultato che, talvolta, i segnalanti allegavano ai loro messaggi fotografie o video che riprendevano veicoli, dei quali fosse visibile la targa di immatricolazione. Pertanto sono stati chiesti al comune elementi di valutazione in ordine alle cautele da adottare, al fine di evitare la diffusione di dati personali non pertinenti ed eccedenti rispetto alla finalità perseguita (nota 11 marzo 2014).

Alla luce di quanto richiesto, il comune ha dichiarato di voler spostare su una piattaforma web, già progettata e in via di acquisizione, la gestione delle segnalazioni che consentirà agli utenti di relazionarsi in maniera riservata con la centrale operativa del comando generale; l'Ufficio ha chiesto di essere informato in merito alla soluzione prescelta, manifestando disponibilità a collaborare (nota 16 giugno 2014).

Impianti elettronici di rilevamento delle violazioni del codice della strada

In relazione poi alla funzione istituzionale comunale dell'accertamento delle violazioni al codice della strada, a seguito di una segnalazione, l'Ufficio ha avuto modo di fornire indicazioni ad un comune sul corretto utilizzo degli impianti elettronici di rilevamento delle infrazioni, sulle modalità con le quali consentire la consultazione sul web delle infrazioni e sulla durata della conservazioni delle immagini a tal fine rilevate. In particolare, è stato evidenziato che l'utilizzo di impianti elettronici di rilevamento automatizzato delle infrazioni è lecito se sono raccolte solo immagini pertinenti e non eccedenti (o inutilmente dettagliate) per il perseguimento della finalità di accertamento del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese.

In particolare, è stato evidenziato che le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (ad es., ai sensi dell'art. 383, d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta) e che, pertanto, deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nel-

l'accertamento amministrativo (cfr. punto 5.3.1. del provvedimento generale). Va evitato, in ogni caso, che tale documentazione video-fotografica riguardante i soggetti non coinvolti sia messa a disposizione del destinatario del verbale di contestazione della violazione.

Al comune è stato quindi richiesto di valutare la pertinenza e non eccedenza dei dati personali contenuti nelle risultanze fotografiche visualizzabili nella pagina web del comune, anche con riferimento ad infrazioni molto risalenti nel tempo, a carico di un determinato numero di targa, nonostante l'avvenuto pagamento della sanzione e l'assenza di contenzioso al riguardo, tenuto anche della circolare del Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 (par. n. 6 dell'All. n. 1), che prevede che "le immagini siano conservate solo per il periodo di tempo strettamente necessario all'applicazione delle sanzioni e alla definizione dell'eventuale contenzioso" (nota 18 luglio 2014). A seguito dell'intervento dell'Ufficio, il comune ha comunicato di aver previsto idonee misure volte ad oscurare le targhe dei veicoli non coinvolti nell'accertamento ma eventualmente oggetto di ripresa e a rimuovere dalla pagina web del comune le immagini relative all'accertamento della violazione, decorso il termine di eventuale presentazione del ricorso decorrente dalla notificazione dell'infrazione al trasgressore (nota 12 dicembre 2014).

Videosorveglianza cd. intelligente

L'Ufficio si è occupato di valutare le richieste di verifica preliminare pervenute in relazione a trattamenti di dati personali effettuati tramite sistemi di videosorveglianza cd. intelligenti.

In particolare, si segnala la richiesta di verifica preliminare formulata dalla Banca d'Italia in relazione ad un sistema destinato ad essere installato presso le sedi dell'amministrazione e delle filiali per garantire la sicurezza degli edifici e dei beni dell'istituto, considerati i rischi specifici connessi allo stoccaggio e alla gestione di elevate quantità di valori.

In primo luogo, è stato verificato che, alla luce di taluni specifici compiti assegnati alla Banca d'Italia (emissione delle banconote in euro e servizio di Tesoreria provinciale e centrale dello Stato), la stessa persegue legittime finalità di sicurezza degli edifici e dei beni, anche attraverso l'istallazione di sistemi di videosorveglianza.

Differenti erano le funzionalità del sistema prospettate dalla Banca d'Italia; al riguardo, è stato precisato che tra le stesse, soltanto quelle di "controllo ambientale" connesse alla generazione di eventi d'allarme a fronte del superamento di una "barriera allarme virtuale", dell'accesso ad una "zona di allarme virtuale", nonché del "riconoscimento presenza persone" comportavano un trattamento di dati personali correttamente sottoposto alla verifica preliminare dell'Autorità in quanto risultavano idonee a rilevare automaticamente, segnalare e registrare comportamenti o eventi anomali, quali possono considerarsi gli accessi nelle zone interdette anche in relazione a determinate fasce orarie (cfr. punto 3.2.1 del predetto provvedimento generale).

L'Autorità ha, invece, ritenuto che altre funzionalità ("lettura targhe e identificazione mezzi", "*motion detection* digitale", "automazione accesso su chiamata citofonica", "conteggio", "riconoscimento oggetto abbandonato" e "mancanza oggetto") non rientrassero tra le ipotesi previste dal provvedimento generale in cui è necessario sottoporre i sistemi di videosorveglianza alla verifica preliminare. Ciò in quanto, per le funzioni di "lettura targhe e identificazione mezzi", "*motion detection* digitale", "automazione accesso su chiamata citofonica" e "conteggio" non è prevista la generazione di allarmi; in relazione alle funzioni di "riconoscimento oggetto abbandonato" e "mancanza oggetto", che prevedono, rispettivamente, l'attivazione di un allarme se un oggetto viene abbandonato all'interno dell'inquadratura di una o più telecamere per un determinato periodo di tempo e se un oggetto esistente viene rimosso dall'inquadratura, non riguardando persone, non comportano un trattamento di dati personali.

Analizzando, allora, nel merito il trattamento dei dati personali effettuato mediante le funzioni correttamente sottoposte alla verifica preliminare dell'Autorità, il Garante lo ha ritenuto proporzionato e quindi ammissibile, non riscontrando, in concreto, un pregiudizio rilevante per gli interessati, tale da determinare effetti particolarmente invasivi sulla loro sfera di autodeterminazione e, conseguentemente, sui loro comportamenti. Le caratteristiche specifiche dei sistemi in esame, infatti, nel rilevare il superamento di una barriera virtuale, delimitata da una linea predefinita, e l'accesso ad una zona interdetta segnalata da idonei cartelli informativi e dispositivi di delimitazione delle zone protette nonché il procedere nel senso contrario in un percorso predefinito, producevano il solo effetto di richiamare l'attenzione degli addetti al posto di controllo, al fine di favorirne un eventuale tempestivo intervento, volto a verificare la fondatezza della segnalazione d'allarme.

Infatti, dalla documentazione trasmessa era risultato che tali sistemi di videosorveglianza non attivavano ulteriori funzionalità, anche eventualmente legate al comportamento dell'interessato ripreso, quali l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali, anche biometrici, o il confronto con una campionatura precostituita.

L'Autorità ha, tuttavia, richiamato l'attenzione della Banca d'Italia sulle prescrizioni relative alle misure minime di sicurezza, con particolare riferimento all'obbligo di adottare specifici accorgimenti tecnici ed organizzativi che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (cfr. punto 3.3.1 del provvedimento generale; artt. 31-36 del Codice e All. B. al Codice), nonché sulle indicazioni in materia di informativa gli interessati (cfr. punto 3.1. del citato provvedimento generale; art. 13 del Codice). Inoltre, sebbene, secondo quanto dichiarato, i sistemi di videosorveglianza in esame non fossero in alcun modo finalizzati ad un controllo dell'attività dei lavoratori, qualora tale attività di videosorveglianza potesse in concreto aver luogo (pur non essendo a tal fine preordinata) il Garante ha evidenziato l'esigenza del rispetto delle garanzie previste per i lavoratori (punto 4.1; art. 114 del Codice; art. 4, l. n. 300/1970) (provv. 22 maggio 2014, n. 259, doc. web n. 3230814).

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

Nel caso di una segnalazione concernente una videoregistrazione di una seduta del consiglio comunale da parte di un consigliere senza aver previamente fornito ai presenti le informazioni di cui all'art. 13 del Codice, è stato evidenziato che il testo unico delle leggi sull'ordinamento degli enti locali stabilisce espressamente che gli atti e le sedute del consiglio comunale e delle commissioni sono pubblici, salvi i casi previsti dal regolamento. Pertanto, spetta all'amministrazione comunale introdurre eventuali limiti a detto regime di pubblicità, mediante un atto di natura regolamentare (artt. 10 e 38, d.lgs. 18 agosto 2000, n. 267). Nell'ipotesi in cui sia prevista la possibilità di effettuare le registrazioni video delle sedute del consiglio comunale, si evidenzia la necessità che agli interessati sia fornita, da parte del comune, l'informativa prevista dall'art. 13 del Codice (nota 3 aprile 2014).

L'Ufficio è intervenuto in più occasioni a seguito di segnalazioni concernenti le modalità di apertura e protocollazione della corrispondenza indirizzata nominativamente a consiglieri comunali presso il comune di appartenenza. In un caso si trattava di corrispondenza proveniente dalla Soprintendenza dei beni e delle attività culturali e del turismo, trasmessa in riscontro ad un esposto presentato dallo stesso consigliere comunale. In un altro caso, la consegna di una nota del Ministero del-

l'interno aperta, protocollata e con la busta spillata, perveniva in risposta ad un quesito del consigliere relativo alla eventuale ineleggibilità di un dipendente dell'unione di comuni alla carica di sindaco di uno degli enti facenti parte dell'unione. In entrambe le occasioni si è ritenuta la correttezza delle procedure operative osservate dal personale addetto all'apertura, protocollazione e distribuzione della corrispondenza in conformità alle specifiche regole stabilite nei manuali di gestione del protocollo informatico, della gestione dei flussi documentali e dell'archivio, approvati dai predetti comuni. Nei predetti casi, inoltre, la corrispondenza era inerente allo svolgimento delle funzioni istituzionali dei consiglieri comunali e non aveva carattere personale, attenendo alla sfera pubblica e alla carica rivestita, e non alla vita privata degli stessi (note 11 giugno e 1° settembre 2014).

Raccolta differenziata dei rifiuti solidi urbani

È tornata di grande attualità la tematica relativa al trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti solidi urbani; ciò ha richiesto l'intervento dell'Ufficio, il quale, su impulso di cittadini o associazioni di consumatori e di amministratori di condominio, ha ricordato le prescrizioni contenute nel provvedimento generale del 14 luglio 2005 (doc. web n. 1149822).

In particolare, in relazione all'utilizzo di sacchetti trasparenti per la raccolta differenziata cd. porta a porta, è stata richiamata l'attenzione sulla prescrizione che considera, in termini generali, non proporzionato l'obbligo di utilizzare un sacchetto trasparente nella raccolta porta a porta, in quanto chiunque si trovi a transitare sul pianerottolo o nell'area antistante l'abitazione può visionare agevolmente il contenuto del sacchetto (note 23 maggio e 4 luglio 2014). In un caso, un comune ha fornito riscontro a quanto richiesto dall'Ufficio, comunicando di aver provveduto a sostituire le forniture dei sacchetti trasparenti utilizzati per la raccolta differenziata.

Sullo stesso argomento, l'Ufficio ha avuto occasione di chiarire in quale caso debba ritenersi applicabile il citato provvedimento del Garante, tenuto conto della diversità delle tipologie di sacchetti e della loro qualificazione (opachi, trasparenti, semi-trasparenti, translucidi): è stato, infatti, precisato che il provvedimento generale del 2005, volto a bilanciare il rispetto della disciplina sulla raccolta differenziata e il diritto degli interessati a non subire violazioni ingiustificate della propria sfera di riservatezza, trova applicazione qualora i sacchetti utilizzati nella raccolta porta a porta siano idonei a mostrare il contenuto degli stessi e, in particolare, effetti personali, che sono talvolta relativi ad informazioni concernenti la sfera della salute o di natura politica, religiosa o sindacale degli interessati (nota 2 gennaio 2015).

In un'altra circostanza, invece, non è stata ravvisata una violazione della disciplina in materia di protezione dei dati personali nel caso di un comune che aveva previsto un servizio telefonico per richiedere la raccolta a domicilio di pannolini e pannoloni per incontinenti e portatori di handicap, in quanto tale previsione costituiva una modalità di prelievo dei citati rifiuti attivabile solo a richiesta degli interessati; dalla documentazione in atti, infatti, non risultava che tale servizio gratuito fosse obbligatorio o esclusivo, essendo contemplata la possibilità che i suddetti materiali potessero essere versati nei sacchetti o nei bidoni riservati ai rifiuti appartenenti alla tipologia "secco residuo non riciclabile" (nota 23 maggio 2014).

Ad una associazione che segnalava la presunta violazione della normativa in materia di protezione dei dati personali da parte di un comune che imponeva per la raccolta dei rifiuti dei sacchetti contenenti un *microchip* identificativo, è stato ricordato che deve ritenersi lecito fornire agli utenti appositi sacchetti, da utilizzare obbligatoriamente per una determinata tipologia di materiale, dotati di *microchip* o, eventualmente, di dispositivi *Radio frequency identification* (Rfid) collegati ai dati identificativi del soggetto cui il contenitore si riferisce. Tale procedura consente di delimitare l'i-

dentificabilità del conferente ai soli casi in cui sia stata accertata la mancata osservanza delle prescrizioni in ordine alla differenziazione. Infatti, al momento dell'apertura del sacchetto, i soggetti preposti alla verifica dell'omogeneità dei materiali inseriti, che comunque sono tenuti al rispetto della riservatezza, vengono a conoscenza del contenuto, ma non anche, in prima battuta, degli elementi identificativi del soggetto conferente. Invece, i soggetti preposti all'applicazione della sanzione, mediante la decodifica del codice a barre o del *microchip*, acquisiscono il nominativo del soggetto cui il sacchetto si riferisce, solo in relazione alla non conformità del contenuto del sacchetto (cfr. punto 4.*c*) del citato provvedimento generale) (nota 25 giugno 2014).

L'Ufficio ha altresì risposto ad un quesito formulato da una università in merito alla possibilità di comunicare ad una società partecipata da più comuni che svolge servizi pubblici locali in materia ambientale dati personali di taluni studenti che si ritenevano essere responsabili dell'abbandono di rifiuti sul suolo pubblico a seguito dei festeggiamenti di laurea, in quanto i nomi degli stessi comparivano nei cartelloni esposti durante i suddetti festeggiamenti. In tale circostanza l'Ufficio ha rilevato un principio, già evidenziato nel provvedimento generale del 2005, secondo il quale 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), avendo cura di esercitare tale riconosciuta facoltà 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 rinvenire elementi in grado di identificare, presuntivamente, il conferente. L'attività di ispezione non costituisce strumento di per sé risolutivo per accertare l'identità del soggetto produttore e il trasgressore non dovrebbe essere individuato sempre ed esclusivamente attraverso una ricerca nei rifiuti di elementi a lui riconducibili; una eventuale sanzione amministrativa irrogata ad un soggetto così individuato potrebbe quindi risultare erroneamente comminata (cfr. punto 4.*d*) del provvedimento generale). Pertanto, la società che svolge servizi pubblici locali in materia ambientale può svolgere l'attività di controllo prevista dalla soprarichiamata l. n. 689/1981 nel rispetto dei limiti indicati nel citato provvedimento generale (nota 8 gennaio 2014).

4.10. *Le comunicazioni di dati personali tra soggetti pubblici*

Il Garante è stato consultato dall'Autorità per le garanzie nelle comunicazioni in merito alla possibilità di avvalersi delle modalità previste dall'art. 58, comma 2, del Cad per la fruibilità informatica di dati presenti nell'Anagrafe tributaria, al fine di verificare la correttezza delle dichiarazioni rese ai sensi degli artt. 46 e 47, d.P.R. 28 dicembre 2000, n. 445, nell'ambito della funzioni di controllo connesse alla tenuta del Registro degli operatori di comunicazione (istituito con l. 5 agosto 1981, n. 416, Disciplina delle imprese editrici e provvidenze per l'editoria), il cui scopo principale è quello di dare trasparenza agli assetti proprietari degli operatori nei settori dell'editoria e della radiotelevisione. L'attestazione da parte del Registro sul controllo (di diritto e di fatto, *ex* art. 2359 c.c.) è richiesta nell'ambito del rilascio delle provvidenze all'editoria erogate dal Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio (l. n. 250/1990 e, da ultimo, d.P.R. n. 223/2010), nel rilascio dei titoli autorizzatori ai fornitori di servizi *media* da parte del MiSE (l. n. 177/2005) e nell'accesso alle provvidenze per le emittenti locali gestite dai Co.Re.Com (l. n. 448/1998).