colloquio con l'Agenzia, o il servizio di Posta elettronica certificata (Pec), utilizzabile in caso di *file* di piccole e medie dimensioni.

La predisposizione dei *file* da trasmettere all'Agenzia dovrà essere effettuata esclusivamente dall'operatore finanziario che non potrà avvalersi di intermediari fiscali.

Tuttavia, poiché l'architettura del sistema non è in grado di escludere eventuali interventi umani (in particolare, nelle operazioni di estrazione dei dati dai sistemi informativi, nonché nella ricezione delle ricevute, soprattutto presso operatori di medie-piccole dimensioni) e prevede la possibilità di passaggi intermedi (nodi di interscambio consorziati) nell'esprimere parere favorevole, il Garante ha chiesto l'adozione di alcune misure di sicurezza, innanzitutto prevedendo che il protocollo Ftp utilizzato per l'intercambio dei dati sia cifrato. L'Autorità ha, inoltre, individuato un'articolata serie di misure, analoghe a quelle già individuate nel citato provvedimento del 17 aprile 2012, che l'Agenzia e gli operatori finanziari dovranno adottare per minimizzare i rischi di accessi abusivi e trattamenti non consentiti e che, per quanto riguarda gli operatori finanziari, dovranno essere inserite nel testo del provvedimento dell'Agenzia. Nel prescrivere queste misure, il Garante ha tenuto conto delle esigenze dei piccoli operatori che non riescono ad automatizzare completamente la procedura e delle ipotesi in cui si avvalgano di nodi di interscambio esterni.

Inoltre l'Agenzia ha previsto che i dati non potranno essere conservati per più di sei anni, allo scadere dei quali saranno automaticamente cancellati.

L'Autorità si è comunque riservata di verificare nel dettaglio il completamento delle funzionalità della nuova infrastruttura informatica, anche prima della messa in esercizio.

Per quanto riguarda infine il provvedimento del Direttore dell'Agenzia con il quale saranno individuati i criteri per la formazione delle liste selettive dei contribuenti a maggior rischio di evasione, l'Agenzia ha dichiarato che sarà sottoposto preventivamente al Garante. L'Autorità ha in ogni caso stabilito che la verifica preliminare sia necessaria per ogni ulteriore utilizzo dei dati ad altre finalità (es. controlli Isee) (parere 15 novembre 2012 [doc. web n. 2099774]).

In seguito, l'Agenzia delle entrate ha rappresentato di voler utilizzare, in luogo della cifratura del protocollo Ftp, (utilizzato per lo scambio dei dati) prescritta dal Garante nel citato parere del 15 novembre 2012, la tecnologia VPN in modalità *site to site*, che assicura la

protezione del canale trasmissivo, su cui viaggiano in chiaro i soli parametri per l'apertura del canale stesso e i comandi Ftp. Il Garante, ritenendo così garantiti livelli di sicurezza non inferiori a quelli derivanti dalla cifratura del protocollo Ftp, ha consentito l'utilizzo di tale tecnologia nei termini prospettati. L'Autorità, inoltre, ha valutato positivamente la scelta dell'Agenzia di introdurre la firma dei *file* anche per le comunicazioni effettuate tramite Pec dagli operatori finanziari (provv. 31 gennaio 2013 [doc. web n. 2268436]).

Partecipazione dei comuni alla lotta all'evasione

L'Autorità ha dato parere favorevole a un schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità tecniche di accesso alle banche dati, di trasmissione di copia delle dichiarazioni relative ai contribuenti e la partecipazione all'accertamento fiscale e contributivo da parte dei comuni, in attuazione della normativa di settore (v. art. 1 del d.l. 30 settembre 2005, n. 203 convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248 e successive modificazioni) (provv. 17 aprile 2012 [doc. web n. 1886825]).

In particolare, il testo, d'intesa con la Guardia di finanza, l'Inps, l'Agenzia del territorio e la Conferenza unificata -fermo restando quanto stabilito dai provvedimenti del Direttore dell'Agenzia delle entrate del 7 dicembre 2007 e del 26 novembre 2008, entrambi sottoposti all'attenzione del Garante (cfr. rispettivamente, pareri 25 luglio 2007 [doc. web n. 1428047] e 30 ottobre 2008 [doc. web n. 1571156])- individua le ulteriori materie per le quali i comuni partecipano all'accertamento fiscale e contributivo e le modalità di accesso alle banche dati.

Il Garante ha espresso parere favorevole su tale schema a condizione che sia integrato al fine di garantire -per tutti i soggetti coinvolti nel trattamento- *standard* di sicurezza minimi non inferiori a quelli garantiti dall'Agenzia delle entrate in conformità al citato provvedimento del 18 settembre 2008.

Nel caso i comuni decidano di avvalersi di eventuali organismi esterni, questi devono essere preventivamente designati quali responsabili del trattamento. I comuni devono fornire adeguate istruzioni in merito al trattamento da effettuare e devono vigilare tramite verifiche periodiche, anche a campione. Qualora tali soggetti siano designati responsabili da più comuni, devono essere garantite misure di carattere tecnico organizzativo volte ad assicurare, nel rispetto degli ambiti territoriali comunali, la separazione logica dei dati e delle banche

dati trattati per conto dei diversi titolari, senza consentire la correlazione tra informazioni di competenza di ciascun comune.

In relazione, invece, alle modalità tecniche di accesso alle banche dati e a quelle di partecipazione dei comuni all'accertamento fiscale e contributivo di competenza, rispettivamente, dell'Agenzia del territorio e dell'Inps, il Garante ha richiesto un'integrazione dello schema che deve essere pertanto sottoposto nuovamente al parere dell'Autorità.

Riscossione

Con riferimento ai trattamenti di dati effettuati a fini di riscossione, il Garante ha prorogato al 30 giugno 2012, su richiesta di Equitalia in accordo con l'Agenzia delle entrate, alcuni degli adempimenti previsti dal provvedimento del 7 ottobre 2009 [doc. web n. 1664231], relativi all'articolazione delle diverse banche dati utilizzate a fini di riscossione, al reperimento delle informazioni anagrafiche da parte delle società del gruppo (a condizione che gli accessi alle anagrafi della popolazione residente effettuati dagli agenti della riscossione avvengano solo in presenza di una iscrizione a ruolo e mediante collegamenti realizzati nel rispetto di idonee misure di sicurezza) e alla predisposizione di attività di controllo, anche attraverso la realizzazione di appositi applicativi, sull'attività svolta dalle società controllate e da Sogei S.p.A. (provv. 12 maggio 2011 [doc. web n. 1822318]).

Secondo quanto rappresentato da Equitalia, infatti, la razionalizzazione dei sistemi informativi e la realizzazione di un nuovo sistema della riscossione hanno richiesto una rimodulazione dei tempi nel conseguimento degli obiettivi, anche in considerazione delle sostanziali modifiche normative intervenute nel 2010 che hanno imposto interventi di aggiornamento significativi. Di conseguenza, anche il processo di monitoraggio statistico di accesso al sistema deve essere riprogrammato con analoga scadenza stante la diretta subordinazione di tale adempimento con quello relativo alla razionalizzazione delle banche dati.

Nel 2012 Equitalia ha quindi dato conto al Garante di aver attuato il complesso processo di riorganizzazione societaria del gruppo, consolidando contestualmente l'infrastruttura tecnologica attraverso il completamento della procedura per la realizzazione di un sistema unico con conseguente razionalizzazione e unificazione delle basi dati. Con riferimento al reperimento delle informazioni anagrafiche da parte delle società del gruppo, Equitalia ha precisato che il nuovo regolamento di gestione dell'Indice nazionale delle anagrafi (decreto

del Ministro dell'interno del 19 gennaio 2012, n. 32), con cui sono state ampliate le informazioni al fine di rendere disponibili alle pp.aa. ulteriori dati anagrafici necessari per l'attività istituzionale, consente di disporre di informazioni complete, attuali e pertinenti. In relazione, invece, alla predisposizione di attività di controllo, il Garante, su richiesta di Equitalia, ha differito al 30 giugno 2013 il termine per gli adempimenti prescritti con il citato provvedimento del 2009, in considerazione dei tempi di progettazione e di avvio della fase sperimentale dei sistemi applicativi di supporto alle attività di controllo (provv. 12 luglio 2012 [doc. web n. 1913804]).

Agenzia delle dogane

L'Agenzia delle dogane ha comunicato all'Autorità l'intenzione di stipulare con l'Unità di informazione finanziaria (Uif) un protocollo che preveda la collaborazione e lo scambio di dati per l'esercizio delle rispettive funzioni istituzionali in materia di controllo sul denaro contante ai sensi del d.lgs. n. 195 del 2008.

In particolare, tale protocollo prevede che l'Agenzia consenta all'Uif, sulla base di specifiche richieste, di accedere alla banca dati relativa ai soggetti che hanno dichiarato trasferimenti di denaro contante.

Con specifico riferimento alle modalità tecniche di scambio di dati tra le autorità competenti, il Garante ha evidenziato che, oltre alle misure minime di sicurezza previste dal Codice, i titolari del trattamento sono tenuti ad adottare misure di sicurezza volte a ridurre al minimo, in particolare, gli accessi non autorizzati o i trattamenti non consentiti e non conformi alle finalità della raccolta.

Pertanto le amministrazioni coinvolte sono state invitate sia ad adottare misure che consentano gli accessi alla banca dati soltanto tramite postazioni di lavoro appartenenti alla rete *Ip* dell'ente autorizzato o/e dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'Agenzia, sia a rendere doverosa l'indicazione da parte dell'operatore dell'Uif del procedimento amministrativo alla base della specifica richiesta. Deve, inoltre, essere predefinita un'idonea procedura per il rilascio e la gestione delle credenziali di autenticazione e delle autorizzazioni con particolare riferimento alla tempestiva disabilitazione degli utenti. La *password*, da comunicare al singolo incaricato separatamente rispetto al codice di identificazione, deve essere modificata dallo stesso al

primo utilizzo e poi periodicamente, bloccando l'utenza a fronte di reiterati tentativi falliti di autenticazione. Le amministrazioni devono poi assicurare l'aggiornamento dei sistemi *software*, dei programmi utilizzati e della protezione antivirus, sia sui *server* che sulle postazioni di lavoro ed introdurre meccanismi volti a garantire che gli accessi avvengano esclusivamente nell'ambito di intervalli temporali o di data predeterminati, definiti sulla base delle esigenze d'ufficio, disciplinando la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone però l'utilizzo ai soli casi necessari per esigenze di servizio. In ogni caso, le operazioni di trattamento dei dati devono essere tracciate e devono essere stabilite periodiche verifiche sugli accessi (nota 26 giugno 2012).

4.6. SISTEMI DI VIDEOSORVEGLIANZA E *RFID* IN AMBITO PUBBLICO

Con riferimento al trattamento di dati personali tramite sistemi di videosorveglianza in ambito pubblico, l'Autorità ha ricevuto numerose segnalazioni, reclami e quesiti in ordine all'applicazione del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (punto 3.2. [doc. web n. 1712680]). Al riguardo molti comuni per disciplinare le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio hanno emanato uno specifico provvedimento, poi trasmesso al Garante per l'approvazione o solo per opportuna conoscenza. Al riguardo l'Autorità ha ribadito che l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo del Garante -fatte salve specifiche ipotesi- e che non può desumersi alcuna approvazione implicita dal semplice inoltro di documenti relativi a progetti di videosorveglianza, cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio assenso. L'Autorità ha inoltre informato i predetti comuni che l'Associazione nazionale comuni italiani (Anci) ha predisposto, con la collaborazione del Garante, linee-guida per fornire alcuni chiarimenti agli enti locali intenzionati ad attivare impianti di videosorveglianza nel territorio (*ex multis* note 7 giugno, 13 settembre, 7 dicembre 2011, 18 ottobre, 29 ottobre, 21 novembre e 20 dicembre 2012).

Più in dettaglio, con reclamo è stato rappresentato che un comune aveva conservato le immagini rilevate tramite un sistema di videosorveglianza per un periodo molto superiore alla

settimana, in quanto aveva potuto fornire nel 2010 ai Carabinieri che le avevano richieste nello svolgimento di indagini di polizia giudiziaria, immagini rilevate nel 2009. Al riguardo, l'Ufficio ha preliminarmente ribadito che la rilevanza e l'ammissibilità in giudizio di atti e documenti basati sul trattamento di dati non conforme alle norme vigenti restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (160, comma 6, del Codice). Con specifico riferimento alla questione oggetto del reclamo, l'Ufficio ha riscontrato invece l'inosservanza del provvedimento generale in materia di videosorveglianza del 29 aprile 2004 [doc. web n. 1003482] -vigente al tempo dei fatti contestati- che limitava ad una settimana la conservazione dei dati personali raccolti (cfr. punto 3.4.) ma non ha ravvisato i presupposti per adottare un provvedimento prescrittivo o inibitorio del Collegio, in quanto la condotta aveva esaurito i suoi effetti ed il comune titolare del trattamento aveva fornito idonee assicurazioni con riferimento alla funzionalità del sistema per cancellare le immagini tramite sovrascrittura delle stesse. In ragione della riscontrata condotta non conforme alla disciplina applicabile sono stati, comunque, avviati gli opportuni accertamenti per l'eventuale contestazione, con un autonomo procedimento sanzionatorio, della violazione amministrativa dell'inosservanza di provvedimenti prescrittivi del Garante (artt. 154, comma 1, lett. *c)* e 162, comma 2-*ter*, del Codice) (nota 26 gennaio 2012).

L'Autorità ha inoltre, ricevuto talune richieste di verifica preliminare alla luce delle indicazioni fornite nel predetto provvedimento generale (punto 3.2.) in particolare il Comune di Firenze ha chiesto la verifica preliminare, ai sensi dell'art. 17 del Codice, con riferimento al trattamento di dati personali relativo al sistema di videosorveglianza cd. "intelligente" che intendeva installare, per finalità di sicurezza urbana, presso la Fontana del Nettuno in Piazza della Signoria, oggetto nel corso degli anni di ripetuti atti vandalici, con ingenti danni al patrimonio pubblico. Tale sistema di videosorveglianza poteva rilevare le coordinate degli oggetti in movimento all'interno della superficie interdetta (consistente nella superficie e colonna d'aria sovrastante la fontana, il verde di bordura e la ringhiera che la circonda), azionare allarmi ottici e visivi individuando e, eventualmente, rilevando i percorsi delle persone e degli oggetti presenti all'interno dell'area stessa. Le immagini rilevate venivano registrate automaticamente in un *server* e conservate per un periodo di sette giorni.

L'Ufficio ha ritenuto corretta la richiesta verifica preliminare trattandosi di sistema di videosorveglianza cd. "intelligente", che non si limita a riprendere e registrare le immagini, ma rileva automaticamente comportamenti o eventi anomali, li segnala e, eventualmente, registra (punto 3.2.1. provv. 8 aprile 2010 [doc. web n. 1712680]). In tale quadro l'Ufficio ha anche rilevato che il trattamento in parola rientra nelle funzioni istituzionali del comune cui spettano specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana per la tutela della quale gli stessi possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico (cfr. art. 54, d.lgs 18 agosto 2000, n. 267; d.m. 5 agosto 2008; art. 6, comma 7, d.l. 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla l. 23 aprile 2009, n. 38). L'Ufficio, alla luce delle motivazioni addotte dal Comune, ha ritenuto proporzionato e ammissibile il trattamento per il rischio del protrarsi degli atti vandalici e dell'elevato valore artistico del monumento, richiamando comunque l'attenzione del Comune stesso sugli adempimenti relativi alle misure di sicurezza ed all'informativa agli interessati (cfr. punto 3.3.1. del cit. provvedimento generale; artt. 13, 31 e 36 del Codice e Allegato B. al Codice) (provv. 7 aprile 2011 [doc. web n. 1811897]).

Ad una provincia che chiedeva se fosse necessario sottoporre alla verifica preliminare un sistema di videosorveglianza da installare presso il palazzo provinciale, l'Ufficio ha evidenziato che spetta alla singola amministrazione valutare se i trattamenti di dati siano riconducibili a quelli che, in base al provvedimento generale, richiedano la verifica preliminare (punto 3.2.1. del cit. provvedimento; art. 17 del Codice) (nota 29 ottobre 2012).

È stato, invece, correttamente sottoposto alla verifica preliminare un sistema di videosorveglianza installato in taluni musei dipendenti dalla Soprintendenza per i beni archeologici di una regione, con riferimento all'intenzione di allungare a trenta giorni i tempi di conservazione delle immagini raccolte, come richiesto dal Comando Legione dei Carabinieri, in considerazione della recrudescenza dei reati contro il patrimonio e dei trafugamenti di opere d'arte. In base agli elementi forniti e alle valutazioni del Comando dei Carabinieri il periodo è stato ritenuto congruo in quanto rispettoso del principio di proporzionalità ma l'allungamento è stato limitato al permanere di tale eccezionale necessità (provv. 18 ottobre 2012 [doc. web n. 2138277]).

Ancora sull'allungamento dei tempi di conservazione delle immagini, l'Ufficio ha precisato a due soggetti pubblici che volevano conservare le immagini registrate, rispettivamente per 5 e 2 giorni, che in base al provvedimento generale del 2010 spetta al titolare del trattamento valutare la sussistenza dei presupposti, quali le peculiari esigenze tecniche o la particolare rischiosità dell'attività, che giustificano la conservazione delle immagini raccolte per un periodo di tempo superiore alle ventiquattro ore e comunque inferiore alla settimana. La verifica preliminare deve essere richiesta al Garante solo se i tempi di conservazione superano una settimana (note 5 e 20 dicembre 2012).

Sempre nell'ambito delle richieste di verifica preliminare, si menziona quella di un comune relativa ad un sistema di videosorveglianza cd. "intelligente" -fornito da una università- per la rilevazione e la segnalazione agli operatori, in maniera automatica e in tempo reale, di eventi critici in alcune aree ritenute sensibili.

Nell'ambito della prima fase del progetto un gruppo di ricerca dell'università si sarebbe occupato di sperimentare, collegandosi al sistema di videosorveglianza cittadino, un applicativo per il rilevamento mediante analisi visuale della presenza di folle, utilizzando unicamente immagini relative ad attori consenzienti. Il comune aveva, quindi, formulato un quesito all'Autorità sulla necessità di sottoporre a verifica preliminare il trattamento dei dati personali di questa prima fase del progetto, precisando che la realizzazione della seconda fase (caratterizzata dall'implementazione delle telecamere intelligenti nel sistema di videosorveglianza cittadino e dall'attivazione delle stesse nelle zone ritenute particolarmente sensibili) sarebbe stata, in ogni caso, preceduta dalla richiesta di verifica preliminare al Garante.

L'Ufficio, nel rispondere al comune, ha evidenziato che essendo nella prima fase il sistema di videosorveglianza intelligente non ancora definito, l'Autorità non era nelle condizioni di individuare idonee misure ed accorgimenti a garanzia degli interessati, non essendo possibile valutare in concreto i rischi del trattamento per i diritti e la dignità degli interessati, in relazione alla specifica finalità perseguita ed al contesto in cui i dati vengono trattati. Pertanto la verifica preliminare è stata ritenuta non necessaria in relazione alla prima fase del progetto.

Essa sarà, invece, necessaria nella seconda fase, poiché al termine della sperimentazione l'Autorità sarà nelle condizioni di valutare gli effetti prodotti dal sistema di videosorveglianza

in relazione, in particolare, alle specifiche finalità perseguite e al contesto in cui il trattamento avrà luogo; elementi, questi ultimi, che il comune dovrà opportunamente evidenziare nell'ambito della predetta richiesta (cfr. punto 3.2.1. provv. 8 aprile 2010, pubblicato in G.U. 29 aprile 2010, n. 99 [doc. web n. 1712680]). Tali indicazioni, fornite dall'Ufficio, sono state sottoposte all'esame del Collegio (nota 22 novembre 2012).

Non è mancata occasione, anche nel 2012, di fornire chiarimenti in merito all'installazione di sistemi di videosorveglianza presso gli istituti scolastici, in particolare in relazione alla lamentata attivazione continua di telecamere all'interno di un istituto e del relativo convitto.

Al riguardo, l'Ufficio ha richiamato il provvedimento dell'8 aprile 2010, nel quale 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 per assicurare l'armonico sviluppo della personalità dei minori. 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 *extra*-scolastiche che si svolgono all'interno della scuola (punto 4.3.1. cit. provv.).

Nelle medesime circostanze, è stato inoltre chiarito che la ripresa di immagini delle aree perimetrali esterne degli edifici scolastici deve essere delimitata alle sole parti interessate, escludendo le aree non strettamente pertinenti l'edificio (punto 4.3.2.); il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (nota 20 dicembre 2012).

È stato altresì ricordato il divieto di controllo a distanza dell'attività lavorativa. Sono infatti vietate l'installazione di apparecchiature preordinate alla predetta finalità nonché le riprese miranti a verificare l'osservanza dei doveri di diligenza e la correttezza nell'esecuzione della prestazione lavorativa (ad es., orientando la telecamera sul *badge*). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature "*dai quali può*

derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lgs. n. 165/2001) (punto 4.1. cit. provv.).

Rfid

Un'altra verifica preliminare è stata richiesta da un comune in relazione al trattamento di dati personali effettuato attraverso un sistema *Rfid (Radio frequency identification)*, per la rilevazione degli orari di ingresso e di uscita dalla zona a traffico limitato (ztl) dei veicoli adibiti al trasporto delle merci per sanzionare i veicoli che si trattengono all'interno della predetta zona oltre l'orario consentito.

Il sistema *Rfid* usa onde elettromagnetiche per l'identificazione automatica di cose o persone, ed è composto di un *tag* (cioè di un'etichetta, dispositivo elettronico di memoria con un codice identificativo unico) e di un lettore utilizzato per leggere tali informazioni. Il Garante con il provvedimento generale del 9 marzo 2005 [doc. web n. 1109493] aveva già individuato specifiche garanzie per l'uso delle cd. "etichette intelligenti" (*Rfid*), riservandosi di prescrivere la verifica preliminare solo per i sistemi *Rfid* destinati all'impianto sottocutaneo.

Il sistema in esame si compone di un'antenna posta su un palo collegata ad una piccola unità locale che registra solo il numero delle targhe dei veicoli autorizzati all'accesso alla ztl, associate al codice univoco con cui il *tag* è identificato dal produttore. Il sistema avrebbe dovuto essere attivo 24 ore su 24, per registrare i *tag* (ingresso e uscita) e consentire di penalizzare i veicoli usciti dalla ztl oltre l'orario consentito. L'Ufficio non ha ritenuto necessaria la verifica preliminare, a garanzia dei diritti degli interessati (art. 7, comma 1, lett. *g)*, del codice della strada), ma ha prescritto, in particolare, che l'informativa (art. 13 del Codice) sia resa all'atto della richiesta del permesso, prima dell'istallazione del sistema *Rfid* sui veicoli autorizzati e, comunque, prima della sua attivazione. Inoltre, in osservanza del principio di necessità (art. 3 del Codice), ha disposto che l'identificazione degli interessati tramite la targa possa essere effettuata solo per l'accertamento della violazione delle regole concernenti gli orari di ingresso e di uscita dalla ztl dei veicoli in parola e per l'applicazione della relativa

sanzione. Con riferimento, poi, ai tempi di conservazione (v. art. 11, comma 1, lett. *e)*, del Codice), il Garante ha prescritto di cancellare le informazioni relative ai veicoli entrati ed usciti dalla ztl nei tempi consentiti subito dopo l'uscita e, in caso di infrazione, di conservare le informazioni rilevate per il solo periodo necessario alla contestazione dell'infrazione stessa, all'applicazione dalla sanzione e alla definizione dell'eventuale contenzioso. Sono state, infine, fornite specifiche indicazioni per garantire la sicurezza dei dati trattati (provv. 2 febbraio 2012 [doc. web n. 1875840]).

4.7. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

L'applicazione della disciplina in materia di protezione dei dati personali in ambito locale e regionale continua a presentare profili problematici.

In relazione alla segnalazione di un'associazione che lamentava una presunta violazione del Codice da parte di una provincia nel quadro di un cd. "Piano territoriale per l'immigrazione" -volto a garantire l'inserimento sociale dei migranti- l'Ufficio ha accertato che non erano mai stati raccolti dati sensibili e le associazioni coinvolte nel progetto venivano correttamente designate responsabili del trattamento. Pertanto non è stata intrapresa alcuna iniziativa (nota 18 ottobre 2012).

Un ulteriore caso ha riguardato l'accesso *online* alla Banca dati dell'emergenza (Bde) istituita dal Comune dell'Aquila, in cui ogni residente può controllare la sua posizione relativamente all'assistenza e alla ricostruzione *post* sisma, tramite l'inserimento di *user id* e *password* individualmente assegnate, previa registrazione con il solo inserimento delle proprie generalità e codice fiscale. L'Ufficio ha rappresentato che per consentire l'accesso ai servizi erogati in rete dal Comune, è necessario l'utilizzo della carta d'identità elettronica e della carta nazionale dei servizi, ovvero di strumenti diversi, purché idonei a consentire l'individuazione informatica del soggetto che richiede il servizio (art. 64, commi 1 e 2, d.lgs. 7 marzo 2005, n. 82). A seguito delle assicurazioni fornite dal Comune relativamente alle procedure di accredito, affinché la consultazione della singola posizione presente in Bde sia univocamente effettuata dall'interessato, l'Ufficio non ha adottato alcun provvedimento (nota 10 dicembre 2012).

Il Garante è stato inoltre interpellato da un comune in ordine alla possibilità di acquisire dagli albergatori -previa adozione di un regolamento per disciplinare il flusso dei dati- le generalità dei turisti che rifiutano di corrispondere la cd. "tassa di soggiorno". Al riguardo l'Ufficio ha chiarito che per la comunicazione non è necessario il consenso degli interessati in presenza di un obbligo stabilito da norme vigenti, ivi compresi i regolamenti (art. 24, comma 1, lett. *a)*, del Codice) (nota 23 agosto 2012).

Sotto un diverso profilo, una cittadina lamentava che il comune di residenza, per emettere la nuova tessera elettorale in sostituzione di quella vecchia priva di spazi per la certificazione del voto, aveva richiesto la restituzione del documento. L'Autorità, considerando che la tessera, riportando l'annotazione della partecipazione al voto, è in grado di rivelare il comportamento elettorale di una persona e, in alcuni casi, l'orientamento politico, ha evidenziato le ragioni della segnalante ed interessato della vicenda il Ministero dell'interno, che ha dato disposizioni alle proprie strutture periferiche di non procedere più in tali casi al ritiro del documento. Questo anche alla luce della normativa in materia, che prevede la restituzione della tessera solo in un numero limitato di ipotesi, tra le quali non rientra l'esaurimento degli spazi per le timbrature (nota 23 agosto 2012).

In un altro caso è stato segnalato che presso il cd. "Sportello unico" per il cittadino di un comune non venivano rispettate le garanzie previste dalla legge a tutela della dignità e della riservatezza delle persone. L'Ufficio ha ribadito al comune che i titolari del trattamento devono a tal fine adottare idonei accorgimenti (cfr. artt. 29 e 30 del Codice), tra i quali, per prevenire l'accesso anche "passivo" ai dati da parte di terzi non autorizzati (ad es., da parte di uno dei componenti la "fila"), l'opportuna istituzione della cd. "distanza di cortesia"(nota 13 dicembre 2012).

In un'altra vicenda, un cittadino ha segnalato che un comune aveva notificato all'interessato una comunicazione in materia urbanistica omettendo di adottare le opportune cautele a tutela della riservatezza, in quanto l'atto in questione non era stato consegnato in mani proprie del destinatario, bensì era stato recapitato a un vicino di casa senza essere inserito in busta sigillata, in violazione dell'art. 174 del Codice. Il comune ha rappresentato che il messo notificatore aveva depositato la comunicazione nell'apposita cassetta delle lettere

dell'interessato e che ignorava come la comunicazione potesse essere finita nella mani di un soggetto estraneo alla procedura.

L'Ufficio, non ravvisando gli estremi di una violazione della disciplina di protezione dati, ha comunque inviato il comune a verificare il rispetto delle citate disposizioni in materia di notificazioni degli atti (nota 25 settembre 2012).

In un altro caso, l'interessato lamentava l'avvenuta notifica a un suo congiunto di una nota con cui si intimava il pagamento dei costi sostenuti dal comune per il ricovero dell'interessato stesso presso strutture assistenziali. Avendo rilevato l'avvenuta comunicazione di dati idonei a rivelare lo stato di salute dell'interessato a terzi, l'Ufficio si è riservato, con autonomo procedimento, di verificare i presupposti per contestare la violazione amministrativa concernente la illegittima comunicazione di dati personali (art. 162, comma 2-*bis*, per violazione dell'art. 20, comma 2, del Codice) (nota 10 dicembre 2012).

Un'altra segnalazione evidenziava che nella documentazione fotografica inviata da un comune a corredo della contestazione di violazione del codice della strada risultavano visibili anche soggetti estranei all'accertamento. Alla luce del provvedimento in materia di videosorveglianza (provv. 8 aprile 2010 [doc. web n. 1712680], in G.U. 29 aprile 2010, n. 99; cfr. Relazione 2009 p. 25 e ss.) in cui è stabilito che la ripresa non deve comprendere soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada), nonché sulla base delle direttive emanate dal Ministero dell'interno, l'Autorità ha prescritto al comune di mascherare per il futuro la porzione delle risultanze video/fotografiche riguardante i soggetti estranei allo specifico accertamento amministrativo (cfr. artt. 143, comma 1, lett. *b)*, e 154, comma 1, lett. *c)*, del Codice). Inoltre, ha vietato al segnalante ogni eventuale trattamento dei dati personali di soggetti non coinvolti nell'accertamento amministrativo, contenuti nella documentazione fotografica speditagli illecitamente dal comune (artt. 143, comma 1, lett. *c)* e 154, comma 1, lett. *d)*, del Codice) (provv. 13 dicembre 2012 [doc. web n. 2185265]).

Si evidenzia, inoltre, il riproporsi di tematiche inerenti il trattamento dei dati da parte di soggetti esterni all'amministrazione comunale, per l'esercizio di funzioni istituzionali (*outsourcing*). In particolare, è stato segnalato che un comune aveva affidato il servizio di noleggio degli autovelox, nonché la gestione delle relative procedure sanzionatorie, a una

società esterna che, a sua volta, aveva affidato a terzi la stampa, l'imbustamento e la spedizione dei verbali di infrazione. In merito, il Garante ha in particolare rappresentato l'esigenza che l'amministrazione -in qualità di titolare del trattamento- designi il soggetto esterno preposto al trattamento come "responsabile del trattamento" con apposito atto scritto che specifichi analiticamente i compiti affidatigli (art. 29 del Codice). In caso contrario, il trattamento di dati personali si configura come una comunicazione esterna, assoggettata alle più stringenti norme previste per tale operazione (art. 19, comma 3, del Codice). Nel caso di specie è stato rappresentato che tutte le società che trattano dati personali per conto del comune dovevano essere nominate responsabili del trattamento da parte del comune e, quindi, anche il soggetto terzo indicato dalla società per l'imbustamento e la stampa dei verbali di infrazione (nota 30 luglio 2012).

4.7.1. Raccolta differenziata dei rifiuti solidi urbani

Nel 2012, il Garante è tornato nuovamente ad interessarsi del trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti solidi urbani.

In particolare, in relazione a tre segnalazioni, nel richiamare le prescrizioni contenute nel provvedimento generale del 14 luglio 2005 [doc. web n. 1149822], è stata esaminata la possibilità che vengano effettuate ispezioni generalizzate del contenuto dei sacchetti per identificare il presunto trasgressore delle prescrizioni relative alla raccolta differenziata dei rifiuti (tipologia di materiale da conferire, specifici giorni o orario di conferimento). Al riguardo è stato evidenziato 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 limitata ai soli casi in cui il soggetto non sia in altro modo identificabile. Risulterebbe, quindi, illegittima la pratica di ispezioni generalizzate da parte del personale incaricato, al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente.

La modalità di accertamento descritta può anche rivelarsi lesiva di situazioni giuridicamente tutelate come la libertà e la segretezza della corrispondenza lasciata nei rifiuti

ed inoltre non sempre risulta agevole, in base agli elementi in esso contenuti, provare la provenienza del sacchetto. Alla luce di tale considerazione si ritiene che il trasgressore non dovrebbe essere individuato sempre ed esclusivamente attraverso una ricerca nel sacchetto dei rifiuti di elementi (corrispondenza o altri documenti) a lui riconducibili, e che quindi una eventuale sanzione amministrativa irrogata ad un soggetto così individuato potrebbe risultare erroneamente comminata (cfr. punto 4. *d)* del citato provvedimento generale) (note 29 ottobre e 5 dicembre 2012).

4.8. COMUNICAZIONI DI DATI PERSONALI TRA SOGGETTI PUBBLICI

Per quanto riguarda la trasmissione di dati fra soggetti pubblici, il Garante ha espresso il parere sullo schema di Accordo tra Ministero della salute, enti locali, province e regioni, sulla prevenzione degli effetti delle ondate di calore, in particolare riguardo alla trasmissione alle Ausl, da parte delle amministrazioni comunali, degli elenchi aggiornati delle persone residenti di età pari o superiore ai 65 anni iscritte nelle anagrafi. Il Garante ha espresso parere favorevole alla trasmissione in quanto la normativa di settore prevede che l'ufficiale di anagrafe possa rilasciare, anche periodicamente, alle amministrazioni pubbliche "*che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità*" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223) elenchi degli iscritti nella Anagrafe della popolazione residente (art. 19, comma 2, del Codice) (provv. 18 maggio 2012 [doc. web n. 1900390]).

Sempre in tema di comunicazione di dati fra soggetti pubblici, si ricorda il caso di un comune che aveva comunicato all'Autorità l'intenzione di fornire indirizzi di residenti e proprietari di immobili, come risultanti dalla banca dati dell'Imposta comunale sugli immobili (Ici), alla soprintendenza per i beni architettonici e paesaggistici di una regione, che ne aveva fatto richiesta, per procedere alla verifica e rinotifica di dichiarazione di interesse culturale (artt. 19, comma 2, e 39, comma 1, del Codice). Al riguardo, alla luce della disciplina di settore (artt. 10 e ss., d.lgs. 22 gennaio 2004, n. 42, "Codice dei beni culturali e del paesaggio"), l'Ufficio non ha formulato osservazioni ostative. È stata comunque richiamata l'esigenza di rispettare i princìpi di pertinenza e di non eccedenza, sensibilizzando il comune in ordine all'esigenza di trasmettere alla suddetta soprintendenza

solo dati strettamente indispensabili per lo scopo istituzionale perseguito (art. 11 del Codice) (nota 8 novembre 2012).

Si segnala inoltre il quesito inoltrato da una Asl in ordine alla richiesta di accesso alla banca dati regionale dell'Anagrafe sanitaria presentata dal Comando Carabinieri-NAS. In merito, il Garante ha ribadito che "*la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia*" è consentita "*per finalità [...] di prevenzione, accertamento o repressione di reati*" (art. 25, comma 2, del Codice). Tuttavia, l'acquisizione per via telematica di dati, informazioni, atti e documenti da parte delle forze di polizia, in conformità alle vigenti disposizioni di legge o di regolamento, rimane subordinata alla stipula di apposite "*convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei princìpi di cui agli articoli 3 e 11*" (art. 54, comma 1, del Codice). Tali "*convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'art. 53*" (art. 54, comma 1, del Codice). In mancanza della suddetta convenzione, la comunicazione dei dati richiesti, con modalità diverse da quella telematica, per esigenze di polizia giudiziaria dal Comando Carabinieri-NAS è possibile soltanto per i dati, pertinenti e non eccedenti, necessari alle finalità di volta in volta rappresentate dalle forze di polizia stesse (nota 27 marzo 2012) (per i pareri espressi dal Garante su alcune convenzioni-tipo; cfr. *infra* par. 8.2.1.).

4.8.1. Il nuovo sistema AVCPass

Il Garante ha espresso parere favorevole sulla deliberazione dell'Autorità per la vigilanza sui contratti pubblici (di seguito Avcp) attuativa dell'art. 6-*bis* del d.lgs. 12 aprile 2006, n. 163 (codice dei contratti pubblici relativi a lavori, servizi e forniture), in base al quale, dal 1° gennaio 2013, le stazioni appaltanti e gli enti aggiudicatori devono verificare il possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per la partecipazione alle procedure disciplinate dal citato codice dei contratti pubblici