Il nuovo strumento di accertamento sintetico è stato sottoposto alla verifica preliminare del Garante perché il calcolo dello scostamento tra i redditi dichiarati e le spese effettuate, utilizzato per selezionare i contribuenti da sottoporre a controlli, è fondato:

- sul trattamento automatizzato di dati personali presenti in Anagrafe tributaria, o comunque conosciuti dall'Agenzia, al fine di selezionare i contribuenti da sottoporre ad accertamento e rideterminarne il reddito sulla base di informazioni comunicate dallo stesso contribuente in ragione di obblighi dichiarativi (ad es., dichiarazione dei redditi, atti del registro) o da soggetti esterni in base ad un obbligo di legge (ad es., operatori telefonici, assicurazioni), nonché altrimenti ricavate dall'Agenzia nell'ambito di specifiche campagne di controllo (ad es., presso *tour operator*, scuole private, *etc.*);
- sull'imputazione al contribuente di spese presunte, quantificate sulla base dell'attribuzione di un profilo (*cluster*) ricavato anche ricorrendo alle ccdd. "spese medie Istat", in relazione alla sua appartenenza ad una specifica tipologia di famiglia e alla residenza in una determinata area geografica.

L'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente, soprattutto se effettuata sulla base delle numerose tipologie di dati posseduti e attraverso l'attribuzione di un profilo, presenta rischi specifici per i diritti fondamentali e la libertà, nonché la dignità degli interessati, che richiedono la previsione di adeguate garanzie. Ciò, in particolare, laddove vengano utilizzate tecniche che rendono possibile collocare gli individui in classi al fine di prendere decisioni sul loro conto (artt. 14 e 17 del Codice).

Il Garante ha esaminato la correttezza e la liceità del trattamento posto in essere dall'Agenzia delle entrate al fine di individuare, in applicazione del Codice, le garanzie da assicurare in relazione alla natura e alla qualità dei dati, alle modalità del trattamento e agli effetti che lo stesso può determinare sugli interessati, introducendo, in particolare, misure e accorgimenti idonei a correggere fattori che generino imprecisioni nei dati, assicurandone l'esattezza e limitando i rischi di errori inerenti alla profilazione, considerato che eventuali imprecisioni nella fase di raccolta di informazioni sono destinate a ripercuotersi, con esiti imprevedibili, sulle determinazioni assunte sulla base di un loro trattamento automatizzato, anche con rilevanti conseguenze in capo agli interessati. Particolare attenzione è stata prestata all'informativa e all'esercizio dei diritti da parte degli interessati, anche nel corso del procedimento amministrativo tributario condotto dall'Agenzia.

La verifica preliminare è stata compiuta anche attraverso accertamenti mirati di carattere ispettivo volti a verificare in concreto il trattamento dei dati contenuti nell'Anagrafe tributaria anche attraverso l'applicativo appositamente realizzato. Nell'ambito di tale procedimento numerose sono state le occasioni di proficuo confronto con l'Agenzia al fine di meglio comprendere le criticità riscontrate e di individuare congiuntamente soluzioni volte a contemperare le esigenze della lotta all'evasione fiscale con il rispetto del diritto alla protezione dei dati personali degli interessati nonché dei principi previsti dal Codice (primo fra tutti quello della qualità dei dati).

Nell'ambito dell'istruttoria sono emersi numerosi profili di criticità che rendevano il sistema non conforme al Codice, derivanti principalmente dal fatto che lo stesso decreto ministeriale di attuazione del nuovo redditometro non era stato sottoposto al previsto parere del Garante, il quale avrebbe così potuto notevolmente anticipare e contribuire a risolvere talune problematiche che, invece, sono emerse solo nel corso della verifica preliminare. Più precisamente, tali criticità hanno riguardato la qualità e l'esattezza dei dati utilizzati dall'Agenzia delle entrate, l'individuazione in via presuntiva della spesa sostenuta da ciascun contribuente riguardo ad ogni aspetto della vita quotidiana (tempo libero, libri, pasti fuori casa, *etc.*) mediante l'attribuzione alla gene-

ralità dei soggetti censiti nell'Anagrafe tributaria della spesa media rilevata dall'Istat, alle informazioni oggetto di esame in contraddittorio con l'Agenzia e all'informativa da rendere al contribuente, con particolare riguardo alle conseguenze sul mancato conferimento dei dati in tutte le fasi del procedimento amministrativo.

Alcune di queste criticità sono state risolte già nel corso della verifica preliminare mediante i correttivi apportati dall'Agenzia delle entrate, anche su indicazione dell'Ufficio. Ulteriori misure a garanzia dei contribuenti sono state quindi prescritte dall'Autorità con il provvedimento del 21 novembre 2013, n. 515 (doc. web n. 2765110).

In particolare, il Garante ha ritenuto che il decreto ministeriale, nella parte in cui prevede la profilazione del contribuente attraverso l'imputazione presuntiva di elementi di capacità contributiva relativi ad ogni singolo aspetto della vita quotidiana – il cui contenuto induttivo è determinato mediante l'utilizzo di spese medie (e, in particolare, di quelle rilevate a fini statistici dall'Istat), non finalizzate alla valorizzazione di un elemento di capacità contributiva certo, e quindi non ancorate all'esistenza di un bene o un servizio e al relativo mantenimento – costituisca un'ingerenza ingiustificata nella vita privata degli interessati in quanto sproporzionata rispetto alle legittime finalità di interesse generale perseguite dall'Agenzia. Ciò va oltre quanto necessario per ricostruire sinteticamente il reddito del contribuente ai sensi dell'art. 38, d.P.R. n. 600/1973 e si pone in contrasto con i principi di correttezza e liceità del trattamento nonché di esattezza dei dati, specie per i profili relativi all'attribuzione delle spese Istat (artt. 2 e 11 del Codice).

Ugualmente, ad avviso del Garante, la circostanza di dover discutere dell'ammontare delle voci di spesa riguardanti ogni singolo aspetto della vita quotidiana con l'amministrazione finanziaria – come proposto dall'Agenzia quale correttivo per circoscrivere l'inesattezza del trattamento derivante dall'utilizzo presuntivo delle spese medie Istat – espone il contribuente a una forte invasione della propria sfera privata, trovandosi lo stesso obbligato a dover giustificare di aver o, soprattutto, non aver sostenuto certe tipologie di spesa, anche relative alle sfere più intime della personalità (cfr. ad es., tempo libero, istruzione dei figli, *etc.*) e a portare a conoscenza nel dettaglio il funzionario dell'Agenzia del proprio stile di vita. Pertanto, a fronte delle criticità evidenziate nell'istruttoria, l'Autorità ha rilevato che anche la raccolta in contraddittorio da parte dell'Agenzia di informazioni relative ad ogni singolo aspetto della vita quotidiana a fini di controllo fiscale, anche risalente nel tempo, seppur effettuato per una rilevante finalità di interesse pubblico, entra in conflitto con i principi in materia di riservatezza e protezione dei dati personali e, in particolare, con l'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali il quale, come noto, prevede che, in una società democratica, l'ingerenza di una autorità pubblica nella vita privata e familiare dell'individuo, ancorché prevista dalla legge, debba essere necessaria e proporzionata.

Alla luce di queste considerazioni, possono così riassumersi le misure che il Garante ha prescritto all'Agenzia delle entrate per rendere il nuovo redditometro conforme al Codice:

- (Profilazione) il reddito del contribuente può essere ricostruito utilizzando unicamente spese certe e spese che valorizzano elementi certi (possesso di beni o utilizzo di servizi e relativo mantenimento) senza utilizzare spese presunte basate unicamente sulla media Istat;
- (Spese medie Istat) i dati delle spese medie Istat non possono essere utilizzati per determinare l'ammontare di spese frazionate e ricorrenti (es., abbigliamento, alimentari, alberghi, *etc.*) per le quali il fisco non ha evidenze certe. Anche sulla base di elementi forniti dall'Istat, è emerso che tali dati, riferibili

allo *standard* di consumo medio familiare, non possono essere ricondotti correttamente ad alcun individuo, se non con notevoli margini di errore, in eccesso o in difetto;

- (Fitto figurativo) il cd. fitto figurativo (attribuito al contribuente in assenza di abitazione in proprietà o locazione nel comune di residenza) non deve essere utilizzato per selezionare i contribuenti da sottoporre ad accertamento, ma solo ove necessario a seguito del contraddittorio. Il fitto figurativo dovrà essere attribuito solo una volta verificata la corretta composizione del nucleo familiare presso l'anagrafe, per evitare le notevoli incongruenze riscontrate dal Garante (che comportavano, ad es., l'attribuzione automatica a 2 milioni di minori della spesa fittizia per l'affitto di una abitazione);
- (Esattezza dei dati) l'Agenzia deve porre particolare attenzione alla qualità e all'esattezza dei dati al fine di prevenire e correggere le evidenti anomalie riscontrate nella banca dati o i disallineamenti tra famiglia fiscale e anagrafica. La corretta composizione della famiglia è infatti rilevante per la ricostruzione del reddito familiare, l'individuazione della tipologia di famiglia o l'attribuzione del cd. fitto figurativo;
- (Informativa ai contribuenti) il contribuente deve essere informato, attraverso l'apposita informativa allegata al modello di dichiarazione dei redditi e disponibile anche sul sito dell'Agenzia delle entrate, del fatto che i suoi dati personali saranno utilizzati anche ai fini del reddirometro. Nell'invito al contraddittorio devono essere specificati chiaramente al contribuente i poteri utilizzati dall'Agenzia delle entrate nell'ambito del trattamento dei suoi dati personali effettuato ai fini di accertamento sintetico ai sensi del citato art. 38, chiarendo la natura obbligatoria o facoltativa degli ulteriori dati richiesti dall'Agenzia (es. dati finanziari) e le conseguenze di un eventuale rifiuto anche parziale a rispondere;
- (Contraddittorio) dati presunti di spesa, non ancorati ad alcun elemento certo e quantificabili esclusivamente sulla base delle spese Istat relativi ad ogni aspetto della vita quotidiana, anche risalenti nel tempo, non possono costituire oggetto del contraddittorio.

**Comunicazioni all'Anagrafe tributaria**

Il Garante ha esaminato lo schema di provvedimento del direttore dell'Agenzia delle entrate in materia di comunicazioni all'Anagrafe tributaria dei dati relativi ai contratti e ai premi assicurativi e volto a riunire in un unico tracciato *record* comunicazioni relative ai premi assicurativi versati e ai dati dei contratti di assicurazione, semplificando le trasmissioni effettuate dalle compagnie di assicurazione e da altri soggetti del settore ed evitando ogni rischio di duplicazione dei dati.

Nel corso dell'istruttoria l'Autorità ha approfondito la questione anche attraverso un accertamento di carattere ispettivo presso l'Agenzia delle entrate al fine di acquisire ogni informazione utile a valutare la pertinenza e la non eccedenza delle informazioni raccolte relative alla voce "contributo al Servizio sanitario nazionale" del tracciato *record* che le compagnie di assicurazione e altri soggetti del settore avrebbero dovuto trasmettere all'Anagrafe tributaria, rispetto alle finalità di controllo formale degli oneri deducibili perseguite dalla norma, anche tenuto conto dei dati relativi alle assicurazioni e ai beni mobili registrati già presenti in Anagrafe tributaria, o comunque disponibili all'Agenzia delle entrate. In particolare, è stata verificata la pertinenza rispetto:

- alla richiesta dei dati relativi all'importo del premio, alla targa del mezzo e alla potenza del motore (Kw/CV) a fronte delle informazioni già rilevabili dal pubblico registro automobilistico, nonché da altre comunicazioni all'Anagrafe tributaria;

- ai dati raccolti sulla base del provvedimento del direttore dell'Agenzia delle entrate del 20 aprile 2012 che prevede la trasmissione telematica della comunicazione degli importi annualmente versati alle province relativi ai contratti di assicurazione contro la responsabilità civile;
- alla soglia prevista per la deducibilità di tale contributo alla luce delle recenti modifiche normative introdotte dall'art. 4, comma 76, l. n. 92/2012, che ne hanno limitato la rilevanza ai soli casi in cui l'importo sia superiore a euro 40.

In relazione agli autoveicoli è risultato quindi possibile limitare la comunicazione – rispetto a quanto inizialmente previsto – ai campi strettamente necessari relativi all'identificativo del contratto di polizza, alla data di stipula del contratto, all'oggetto del contratto e alla targa del veicolo, in quanto i dati relativi alla potenza del motore e all'ammontare totale del premio possono essere acquisiti, rispettivamente, dal pubblico registro automobilistico e dai dati comunicati all'Anagrafe tributaria dalle assicurazioni ai sensi del provvedimento del Direttore dell'Agenzia del 20 aprile 2012, relativo ai soli veicoli a motore.

Con riferimento alla soglia prevista per la deducibilità del contributo al Ssn, introdotta dall'art. 4, comma 76, l. n. 92/2012, l'Agenzia ha ritenuto altresì di poter limitare l'obbligo di comunicazione ai casi in cui l'importo sia superiore a euro 40, modificando il tracciato record affinché risulti chiaro che, nel caso in cui il contributo sia inferiore a detta soglia, gli elementi dell'intero tracciato non devono essere compilati.

Riguardo alle modalità tecniche di scambio dei dati, considerato che lo schema ha previsto che i soggetti obbligati effettuino le comunicazioni previste utilizzando il servizio telematico Entrarel o Fisconline, già oggetto di rilievi critici del Garante con il provvedimento del 17 aprile 2012, n. 145 (doc. web n. 1886775), l'Agenzia ha dichiarato che tali comunicazioni saranno trasferite sulla nuova infrastruttura Sistema di interscambio dati (Sid) in corso di realizzazione, già valutato favorevolmente del Garante nel parere del 15 novembre 2012, n. 861 (doc. web n. 2099774) e nel provvedimento del 31 gennaio 2013, n. 48 (doc. web n. 2268436), e che, comunque, sono stati pianificati alcuni interventi evolutivi del servizio telematico Entratel riferiti, in particolare, alla gestione della dimensione dei *file* e al monitoraggio dell'utilizzo delle credenziali di accesso.

Il Garante, pertanto, a seguito delle modifiche apportate, ha espresso parere favorevole sulla successiva versione dello schema di provvedimento predisposta dell'Agenzia, che ha tenuto conto degli approfondimenti richiesti dall'Ufficio relativi alla pertinenza e non eccedenza dei dati, a condizione che tali comunicazioni fossero trasferite sulla nuova infrastruttura Sid entro il 31 dicembre 2013 (provv. 4 aprile 2013, n. 153, doc. web n. 2462488).

**Accesso all'Archivio dei rapporti finanziari**

L'Agenzia delle entrate ha chiesto al Garante chiarimenti in ordine ad una sentenza del Tar Lazio del 21 ottobre 2013, n. 9036, secondo cui, tra i "documenti fiscali" che l'Agenzia delle entrate dovrebbe esibire ad un ricorrente ai sensi della l. n. 241/1990, rientrerebbero anche le "comunicazioni inviate da tutti gli operatori finanziari dell'Anagrafe tributaria – sezione Archivio dei rapporti finanziari – relative ai rapporti continuativi, alle operazioni di natura finanziaria ed ai rapporti di qualsiasi genere".

In relazione a quanto rappresentato dall'Agenzia, l'Autorità ha deciso di dare mandato all'Avvocatura dello Stato per impugnare la sentenza e ha evidenziato in un'apposita nota alla stessa Agenzia, oltre a più generali criticità in ordine all'applicabilità del concetto stesso di documento amministrativo a tal genere di banca dati, che una simile applicazione della disciplina sull'accesso ai documenti amministrativi si pone in contrasto con i diritti e le libertà fondamentali nonché con la dignità

degli interessati, beni tutelati dalla normativa, anche di rilevanza comunitaria, in materia di protezione dei dati personali, specie con riferimento all'eccezionale concentrazione presso l'Archivio dei rapporti finanziari (che costituisce un'apposita sezione separata dell'Anagrafe tributaria) di un'enorme quantità di informazioni personali riferibili alla totalità dei contribuenti, con ciò snaturando le specifiche ed emergenziali finalità di contrasto all'evasione fiscale che hanno legittimato la costituzione di tale banca dati.

Dalla documentazione disponibile al Garante, risulta infatti che l'Archivio dei rapporti finanziari contenga circa 600.000.000 (seicento milioni) di rapporti attivi e che annualmente gli operatori finanziari effettuano circa 155.000.000 (centocinquantacinque milioni) di comunicazioni relative alle sole variazioni dei rapporti in essere e alle cd. operazioni extraconto.

La legge stabilisce tassativamente i soggetti e le specifiche finalità per cui tali dati possono essere utilizzati. Ad esempio, oltre all'autorità giudiziaria e per specifiche finalità antimafia e antiterrorismo, l'Agenzia può farvi accesso unicamente a seguito dell'avvio di indagini finanziarie per le attività connesse all'accertamento sulle imposte dei redditi e sul valore aggiunto ed alla riscossione mediante ruolo, nonché, con riferimento ai cd. dati contabili raccolti a partire dal 2011, unicamente con modalità centralizzate per la formazione di liste selettive di contribuenti a maggior rischio evasione.

Estendere l'utilizzo delle informazioni contenute nelle comunicazioni degli operatori finanziari all'Archivio dei rapporti in assenza dei (e, quindi oltre, i) predetti presupposti soggettivi e oggettivi tassativamente individuati dal legislatore come prefigurato dalla citata sentenza del Tar del Lazio significherebbe, di fatto, equiparare il penetrante potere d'indagine dell'Agenzia delle entrate e quello riservato all'accertamento di fattispecie penalmente rilevanti a quello di chiunque risultasse portatore di un interesse e quindi anche di altri innumerevoli soggetti (pubbliche amministrazioni e imprese). Con ciò superando i limiti imposti dal legislatore nella costituzione di tale Archivio ed esponendo la totalità dei contribuenti ad una sproporzionata invasione della propria vita privata, in conflitto con la necessità di rispettare i limiti posti dai principi in materia di riservatezza e protezione dei dati personali e, in particolare, dall'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (nota 20 dicembre 2013).

### 4.8. *La videosorveglianza in ambito pubblico*

Anche nel corso del 2013, frequenti richieste si sono incentrate sulla necessità di sottoporre (o meno) alla verifica preliminare dell'Autorità sistemi di videosorveglianza (come previsto nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010, doc. web n. 1712680).

**Riconoscimento facciale e veicolare**

A tal riguardo, in presenza di una richiesta di autorizzazione e di verifica preliminare ai sensi dell'art. 17 del Codice da parte di un comune in relazione al trattamento di dati personali che intendeva effettuare tramite sistemi di videosorveglianza intelligenti "con riconoscimento facciale e veicolare dei trasgressori", per controllare il deposito di rifiuti domestici in orari non consentiti nonché di rifiuti ingombranti, inquinanti e pericolosi, al fine di procedere alla relativa contestazione dei verbali di violazione, l'Ufficio ha fornito alcuni chiarimenti in ordine all'autorizzazione e ha manifestato l'esigenza di conoscere taluni elementi utili alla istruttoria (tra i quali la modalità di funzionamento del sistema di riconoscimento delle caratteristiche fisionomiche degli interessati, l'eventuale collegamento, incrocio o confronto con altri dati perso-

nali, il contesto in cui il predetto sistema sarebbe stato installato nonché l'eventuale capacità dello stesso di rilevare i percorsi degli interessati). Poiché gli elementi forniti dal comune non risultavano rientrare tra le ipotesi individuate nel provvedimento generale del 2010 in cui è necessario sottoporre i sistemi di videosorveglianza alla verifica preliminare dell'Autorità, non è stato dato seguito alla richiesta (note 13 settembre 2013 e 8 gennaio 2014).

Un'azienda di trasporti, *partner* di un progetto europeo volto a sviluppare un sistema di sicurezza del trasporto pubblico nelle città europee, ha chiesto la verifica preliminare per i trattamenti di dati personali effettuati tramite sistemi di videosorveglianza "intelligenti" ideati per la realizzazione del progetto. A seguito di un incontro svoltosi presso l'Ufficio, è stato precisato che, in realtà, si sarebbero realizzate soltanto delle rappresentazioni con attori consenzienti e che l'azienda non avrebbe, quindi, trattato alcun dato personale dei passeggeri del trasporto pubblico. Nel prendere atto di quanto dichiarato, l'Ufficio ha comunicato l'archiviazione della richiesta (nota 26 giugno 2013).

**Monitoraggio del traffico acqueo**

Anche la Città di Venezia ha formulato una richiesta di verifica preliminare in ordine ad un sistema di videosorveglianza denominato "Argos" volto a monitorare la navigazione nei rii, canali e tratti più interessati dal traffico acqueo. Al fine di acquisire elementi necessari all'esame dei sistemi da utilizzare, sono stati avviati contatti per le vie brevi e richiesti chiarimenti, anche in vista di un incontro da tenersi presso la sede dell'Ufficio. Alla luce delle indicazioni fornite, il trattamento dei dati personali non è risultato da qualificare tra quelli da sottoporre alla verifica preliminare dell'Autorità.

**Grande Progetto Pompei**

È stato dato seguito, invece, ad una richiesta di verifica preliminare presentata dalla Soprintendenza Speciale per i beni archeologici di Napoli e Pompei in relazione all'intenzione di allungare i tempi di conservazione delle immagini raccolte tramite il "Sistema di videosorveglianza dell'area archeologica di Pompei". La Soprintendenza ha sottoposto al Garante la richiesta di prolungamento del periodo di conservazione delle immagini registrate mediante talune telecamere dedicate a sorvegliare i cantieri e le aree di stoccaggio del "Grande Progetto Pompei" nonché i varchi di accesso riservati al transito del personale e dei mezzi diretti ai cantieri medesimi, per un periodo superiore alla settimana, presentando, a supporto di tale istanza, una richiesta della Direzione investigativa antimafia - Centro operativo di Napoli. Al riguardo, la citata Direzione aveva valutato che l'arco temporale individuato appariva adeguato in considerazione dei tempi occorrenti per il restauro dei diversi siti archeologici, considerato che le relative fasi di fornitura dei materiali o il noleggio di mezzi, normalmente si esauriscono all'interno di tale periodo temporale.

La Soprintendenza Speciale ha dichiarato che l'attività di videosorveglianza interessata dalla verifica preliminare avrebbe supportato l'attività della Prefettura volta a controllare, soprattutto a fini di prevenzione antimafia, la regolarità degli accessi e delle presenze in cantiere e non sarebbe stata quindi finalizzata al controllo dell'attività dei lavoratori.

L'Autorità ha richiamato il provvedimento generale dell'8 aprile 2010 e le speciali disposizioni di legge, entrate in vigore prima della normativa in materia di protezione dei dati personali, che prevedono la possibilità di installare impianti audiovisivi presso i musei statali per il controllo continuativo ed ininterrotto dei beni culturali esposti o depositati, con finalità di prevenzione e di tutela da azioni criminose e danneggiamenti (d.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla l. 14 gennaio 1993, n. 4); considerati quindi gli elementi acquisiti, anche sulla scorta delle valutazioni espresse dalla Direzione investigativa antimafia, è stata ritenuta sussistente una specifica esigenza di sicurezza, in relazione ad una concreta

situazione di rischio. È stato pertanto ritenuto congruo un allungamento dei tempi di conservazione delle immagini per il periodo richiesto, in quanto rispettoso del principio di proporzionalità, che prevede la conservazione dei dati personali oggetto di trattamento, in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (art. 11, comma 1, lett. *e*), del Codice; punto 3.4. del citato provvedimento), pendente la rappresentata eccezionale necessità. È stato comunque precisato che, ove l'attività di sorveglianza dei cantieri consenta, pur non essendovi preordinata, un controllo a distanza dell'attività dei lavoratori, resta ferma l'esigenza che venga rispettato il provvedimento generale del Garante dell'8 aprile 2010, con particolare riferimento alle garanzie previste per i lavoratori dagli artt. 114 del Codice e 4, l. 20 maggio 1970, n. 300 (provv. 3 ottobre 2013, n. 428, doc. web n. 2724840).

**Tempi di conservazione delle immagini**

Analogamente, con riferimento all'istanza presentata da Sogei per ottenere l'autorizzazione all'allungamento dei tempi di conservazione delle immagini videoregistrate presso la sede della società, il Garante ha ammesso la conservazione per trenta giorni delle immagini raccolte attraverso il sistema di videosorveglianza. È stata valutata, infatti, la peculiarità dell'attività di Sogei, che conserva e custodisce nella propria banca dati l'intera Anagrafe tributaria, il cui Sistema Informativo della Fiscalità è fra i più complessi e strategici nell'ambito della p.a.

Il sistema di videosorveglianza descritto ha la finalità di proteggere le banche dati da accessi non autorizzati e di tutelare le apparecchiature *hardware* e i prodotti *software* utilizzati per la loro gestione, nonché i beni e le persone che operano all'interno dei locali e nelle aree aziendali. La richiesta di estendere il periodo di conservazione delle immagini era stata motivata, in particolare, da specifiche esigenze di sicurezza finalizzate a prevenire minacce terroristiche, rischi di intrusione e possibili azioni criminose e in alcun modo finalizzata ad un controllo dell'attività dei lavoratori.

Nell'accogliere la richiesta presentata, il Garante ha tenuto conto della particolare delicatezza e della mole dei dati trattati dall'Anagrafe tributaria nonché delle specifiche esigenze di sicurezza e di protezione di banche dati, beni aziendali e persone, in relazione ad una concreta situazione di rischio, valutata anche dal Ministero dell'economia e delle finanze - Organo centrale di sicurezza (provv. 28 novembre 2013, n. 532, doc. web n. 2803442).

Anche l'Enea (Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile) - Centro ricerche Frascati, ha richiesto al Garante di poter allungare i tempi di conservazione delle immagini raccolte mediante i sistemi di videosorveglianza fino a quarrordici giorni durante i periodi di chiusura del Centro. Tale richiesta è stata motivata sulla base della necessità di impedire l'accesso fraudolento in alcuni locali dove si trovano impianti e/o sostanze potenzialmente nocive per la salute, nonché ulteriori furti di rame, considerato il frequente susseguirsi di tali eventi, da considerarsi "altamente probabili e quindi incombenti".

A sostegno della citata richiesta, l'Agenzia ha rappresentato che nei laboratori del Centro vengono effettuate attività di ricerca e sviluppo di applicazioni delle radiazioni relative a sorgenti laser (a gas, a sraro solido, a elettroni liberi) e applicazioni laser nel campo della diagnostica (ambientale, industriale e medicale) dei nano e micro sistemi, della metrologia e della visione laser; da ciò deriverebbero specifici rischi legati all'utilizzo di sostanze chimiche, gas pericolosi e radiazioni non ionizzanti e, con particolare riguardo alle attività nucleari, anche rischi di eventi delittuosi gravi.

Infine, è stato assicurato che, decorso il periodo di conservazione, le registrazioni verrebbero cancellate e comunque non utilizzate per il controllo a distanza dei dipendenti.

La specifica esigenza di sicurezza, riconnessa alla delicatezza dell'attività di ricerca svolta e ai concreti rischi di sottrazione indebita di materiali ed apparecchiature ha indotto il Garante ad accogliere la richiesta di verifica preliminare relativa all'allungamento dei tempi di conservazione delle immagini registrate dagli impianti di videosorveglianza dall'Enea, chiarendo che l'accesso alle stesse avrebbe potuto essere effettuato solo nel caso in cui fossero ravvisati o segnalati eventuali illeciti oppure in caso di richiesta in tal senso da parte dell'autorità giudiziaria (provv. 11 aprile 2013, n. 178, doc. web n. 2464185).

**Sistemi di videosorveglianza "intelligenti"**

Le richieste di verifica preliminare non hanno riguardato soltanto l'allungamento dei tempi di conservazione delle immagini, ma anche trattamenti di dati personali effettuati tramite sistemi di videosorveglianza cd. "intelligenti". Si fa riferimento, segnatamente, alla richiesta di attivazione da parte di un comune di un particolare sistema di videosorveglianza nell'ambito dell'attività di sicurezza urbana, al fine di evitare atti vandalici e danneggiamenti a monumenti e sedi istituzionali. In particolare, il sistema di videosorveglianza sottoposto all'esame dell'Autorità risultava composto da dieci telecamere, con inquadratura fissa, che avrebbero azionato un allarme, a seguito della rilevazione della permanenza prolungata da parte di un individuo, per oltre 30 secondi, nell'area virtuale contrassegnata da un'immaginaria linea di interdizione adiacente ai siti monumentali, e per oltre 60 secondi, per quella situata in prossimità delle sedi istituzionali. L'allarme, di tipo ottico/acustico, si sarebbe manifestato sul monitor della postazione di controllo, richiamando l'attenzione dell'operatore di polizia locale addetto alla centrale operativa per il quale si sarebbero rese visibili le informazioni dettagliate dell'evento, al fine di consentire un eventuale pronto intervento.

Il sistema descritto, in base al provvedimento del 2010 in materia di videosorveglianza, era stato correttamente sottoposto alla verifica preliminare dell'Autorità, in quanto rientrante tra i sistemi di ripresa "intelligenti" che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli. Il Garante si è quindi espresso evidenziando che il sistema, per le sue caratteristiche, non avrebbe comportato in concreto un pregiudizio rilevante per i diritti e le libertà fondamentali dei cittadini, in quanto, nel rilevare la presenza prolungata degli interessati nell'area adiacente ai monumenti e alle sedi istituzionali, avrebbe avuto come unico effetto quello di richiamare l'attenzione dell'operatore di polizia addetto alla centrale operativa al fine di favorire, se necessario, un tempestivo intervento. Dalla documentazione trasmessa in atti non è risultata l'attivazione di ulteriori funzionalità del sistema, eventualmente legate al comportamento dell'interessato ripreso, quali, ad esempio, la capacità di rilevarne i percorsi, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali o confronto con una campionatura precostituita.

Il Garante ha ritenuto quindi proporzionato il trattamento dei dati personali che il comune intendeva effettuare per le finalità di sicurezza urbana, valutata l'esigenza di tutela dei siti monumentali – già oggetto di atti vandalici – e istituzionali, nonché la dichiarata inadeguatezza delle misure di controllo alternative determinata dall'esiguità del personale a disposizione. L'Autorità ha però richiesto che nell'informativa fossero chiaramente evidenziate le caratteristiche del sistema (con particolare riguardo alla rilevazione e segnalazione della presenza prolungata nelle aree delimitate dalla linea di interdizione virtuale in prossimità delle sedi e degli edifici selezionati), richiamando altresì l'attenzione sulle misure di sicurezza da adottare, al fine di consentire, in particolare, la verifica delle attività sugli accessi alle immagini o sul controllo dei sistemi di ripresa, nonché sulla necessità di rispettare i tempi limitati di conservazione delle immagini registrate (provv. 21 marzo 2013, n. 136, doc. web n. 2380059).

**Sistemi mobili di videosorveglianza**

Sono stati altresì forniti chiarimenti in merito all'installazione di sistemi di videosorveglianza mobili, a seguito di una specifica istanza formulata da un comune che intendeva installare tali sistemi "al fine di combattere efficacemente il dilagante fenomeno dell'abbandono incontrollato di rifiuti (pericolosi e non) nel centro abitato e nelle campagne". Al riguardo è stato rappresentato che l'utilizzo di sistemi di videosorveglianza, anche di tipo mobile, risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli inefficace, il ricorso a strumenti e sistemi di controllo alternativi (cfr. punto 5.2. del provvedimento generale). Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (nota 19 novembre 2013).

Sempre con riferimento a sistemi mobili di videosorveglianza, si menziona la richiesta di chiarimenti da parte del Dipartimento vigili del fuoco-soccorso pubblico e difesa civile in ordine alla possibilità di equipaggiare i veicoli in dotazione, impegnati nel servizio di soccorso tecnico urgente, di un sistema di apparati mobili di videosorveglianza di bordo; ciò consentirebbe la registrazione di flussi audio-video georeferenziali e la trasmissione in tempo reale delle informazioni rilevate alla sala operativa di ciascun Comando provinciale, competente per territorio, e al sistema centrale di gestione ubicato presso il Comando provinciale di Napoli.

Al riguardo, l'Ufficio ha rilevato che talune disposizioni del Codice, tra le quali quella riguardante l'obbligo di fornire una preventiva informativa agli interessati, non sono applicabili al trattamento di dati personali effettuato, anche sotto forma di suoni e immagini, dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, ove effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento (art. 53 del Codice).

Alla luce di tale previsione, è stato rappresentato che per i predetti titolari del trattamento, tra i quali rientrano anche gli appartenenti al Corpo dei vigili del fuoco (art. 8, l. 27 dicembre 1941, n. 1570) quando pongono in essere trattamenti riconducibili a quelli previsti dall'art. 53 del Codice – relativi, ad esempio, al contrasto di atti criminosi compiuti con l'uso di armi nucleari, batteriologiche, chimiche e radiologiche (cfr. art. 24, comma 5, lett. *a*), d.lgs. 8 marzo 2006, n. 139) –, vale la regola secondo la quale l'informativa può non essere resa, sempre che appunto i dati personali siano trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati e il trattamento sia comunque effettuato in base ad espressa disposizione di legge che lo preveda specificamente.

Al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, l'Autorità ha tuttavia ritenuto fortemente auspicabile che l'informativa – benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice – sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati. Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace

funzione di deterrenza; in ogni caso, anche se i titolari si avvalessero della facoltà di fornire l'informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall'art. 53, comma 1, lett. *a*) e *b*).

È stato sottolineato, al contrario, che deve essere fornita un'idonea informativa in tutti i casi in cui i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle Forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (cfr. punti 3.1.1. e 3.1.2. del provvedimento generale del 2010) (nota 5 marzo 2013).

**Videosorveglianza di area marina protetta**

L'Autorità è altresì intervenuta, a seguito di notizie riportate dagli organi di informazione, per verificare la correttezza del trattamento dei dati personali effettuato tramite un sistema di videosorveglianza previsto presso il territorio costiero dell'area marina protetta Penisola del Sinis-Isola di Mal di Ventre da un comune sardo in collaborazione con l'Agenzia conservatoria delle coste della Sardegna; in particolare, sono stati richiesti elementi in ordine alle modalità di configurazione del sistema con le quali si sarebbe inteso garantire il rispetto dei principi di necessità e di proporzionalità sia nella scelta della modalità di ripresa e di dislocazione delle telecamere, sia nelle varie fasi del trattamento, avendo cura di specificare l'eventuale identificabilità dei soggetti ripresi nonché se fosse previsto l'inserimento delle immagini raccolte sulla rete internet (nota 17 giugno 2013). Al riguardo, il comune ha chiarito che le telecamere, ancora da attivare e preordinate a verificare le condizioni meteo-marine nonché a valutare l'erosione costiera, sarebbero state configurate in modo da non consentire di effettuare riprese particolareggiate tali da rendere identificabili i soggetti ripresi.

Sempre in tema di videosorveglianza di aree marine, un comune sardo ha comunicato all'Autorità l'intenzione di installare alcune *webcam* presso spiagge e punti panoramici, con finalità di promozione turistica. Al riguardo, è stato evidenziato che l'attività di rilevazione di immagini a scopi promozionali-turistici deve avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento (punto 4.5 del provvedimento generale del 2010) (nota 22 luglio 2013).

**Limiti di velocità**

L'Ufficio è stato interpellato dal Dipartimento per i trasporti, la navigazione e i sistemi informativi e statistici del Ministero delle infrastrutture e dei trasporti in ordine alla legittimità di un dispositivo per l'accertamento a distanza della violazione del limite di velocità – rispetto al quale aveva ricevuto una richiesta di omologazione – anche attraverso riprese frontali del veicolo con il quale viene commessa l'infrazione. Sul punto, come evidenziato nel corso di un incontro preliminare, sono state richiamate le indicazioni fornite dal Garante nel provvedimento del 2010, precisando che, in conformità al quadro normativo di settore in materia di violazioni al codice della strada, le risultanze video/fotografiche devono contenere solo gli elementi previsti per la predisposizione del verbale di accertamento delle violazioni (tra i quali, il giorno, l'ora e la località nei quali la violazione è avvenuta, le generalità e residenza del trasgressore, la targa di riconoscimento, la sommaria esposizione del fatto, nonché la citazione della norma violata, cfr. art. 383, d.P.R. n. 495/1992); pertanto, devono essere oscurate le immagini rilevate incidentalmente, non pertinenti rispetto alla finalità di predisposizione del verbale di accertamento delle violazioni (nota 25 luglio 2013).

Da ultimo, il Garante è intervenuto in merito alla possibilità che gli organismi sanitari possano usare sistemi di videosorveglianza all'interno dei propri servizi igienici per il controllo della procedura di raccolta del campione urinario per accertare l'assenza di tossicodipendenza a fini certificatori, nonché di cura della salute, individuando talune cautele ed accorgimenti in un provvedimento generale (provv. 15 maggio 2013, n. 243, doc. web n. 2475383), più diffusamente descritto nel par. 5.1.

### 4.9: *I trattamenti effettuati presso regioni ed enti locali*

La disciplina in materia di protezione dei dati personali continua a presentare criticità in ambito locale e regionale.

L'Ufficio è intervenuto con riferimento al quesito sottoposto da un comune in ordine all'utilizzo di apparecchiature video durante la seduta del consiglio comunale. A tal proposito, è stato rappresentato 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 pubbliche, salvi i casi previsti dal regolamento. Pertanto, si è ritenuto che spetti 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) e che non competa all'Autorità sindacare le scelte effettuate con il regolamento nel quale si sono disciplinati i limiti e le modalità di pubblicità delle sedute consiliari. Ove sia consentita l'effettuazione di riprese delle sedute del consiglio comunale, agli interessati deve essere fornita, da parte del comune, l'informativa prevista dall'art. 13 del Codice (nota 1° ottobre 2013).

**Outsourcing nella p.a.**

Si segnala il riproporsi della problematica inerente al trattamento dei dati effettuato da soggetti esterni all'amministrazione comunale per l'esercizio di funzioni istituzionali (*outsourcing*). In particolare, un'associazione di consumatori ha formulato un quesito in ordine alla possibilità per la polizia municipale di affidare al personale di società il trattamento di dati personali effettuato, dopo l'accertamento da parte degli agenti della polizia municipale, di attività quali la digitalizzazione delle immagini derivanti da fotogrammi acquisite da apparecchiature *autovelox*, la stampa delle visure del Pubblico registro automobilistico (Pra), la stampa di verbali, *etc.*

Analogamente sono pervenute segnalazione di cittadini relative alla notifica di verbali di infrazione delle disposizioni del codice della strada a mezzo di società cui vengono affidate dai comuni le attività di stampa, imbustamento e spedizione dei verbali.

In proposito è stato rappresentato che nello svolgimento dei propri compiti istituzionali, ciascun soggetto pubblico, in qualità di titolare del trattamento (art. 4, comma 1, lett. *f*), del Codice), può avvalersi del contributo di soggetti esterni, anche privati (cd. *outsourcing*), affidando a essi determinate attività, che restano nella sfera della titolarità dell'amministrazione stessa, atteso che comportano decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati. Tuttavia, in questa ipotesi, l'amministrazione pubblica titolare del trattamento deve designare il soggetto esterno come "responsabile del trattamento" con un apposito atto scritto che specifichi i compiti affidati e contenga puntuali indicazioni, anche per ciò che riguarda la sicurezza e l'utilizzo dei dati (art. 29, commi 1-5, del Codice). In caso contrario, il trattamento di dati personali si configura come una comunicazione e, in quanto tale, è assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice). Inoltre, è stato precisato che le persone fisiche che materialmente trattano i dati personali devono essere designate "incaricati del trattamento" con un atto scritto che individui puntualmente l'ambito del trattamento che essi possono effettuare (art. 30, comma 1, del Codice) (nota 28 maggio 2013).

In un altro caso, è stata lamentata la notificazione di una comunicazione in materia tributaria da parte di un comune, effettuata su un foglio piegato in tre parti e spillato, al cui esterno erano stati indicati dati personali eccedenti quelli strettamente necessari per la notifica (quali la data di nascita e il codice fiscale della destinataria della missiva). Il Garante ha evidenziato che i dati riguardanti la data di nascita e il codice fiscale degli interessati (ancorché utilizzati dall'Amministrazione procedente, insieme alle altre informazioni anagrafiche detenute, al fine di verificare la sussistenza di eventuali omonimie), non possono essere apposti sulla parte esterna del plico che deve riportare solo le informazioni necessarie alla notificazione della comunicazione del destinatario (cioè nome, cognome e indirizzo). Il trattamento di tali dati oggetto di segnalazione è risultato eccedente e non pertinente rispetto alla finalità perseguita di inoltrare il plico all'indirizzo delle persone cui la comunicazione è diretta, in quanto la condotta segnalata aveva comportato l'ingiustificata conoscenza delle predette informazioni da parte di terzi, in violazione dell'art. 11, comma 1, lett. *d*), del Codice. Pertanto, nel dichiarare illecito il trattamento, il Garante ha prescritto al comune di adottare per il futuro opportune cautele al fine di prevenire la conoscenza ingiustificata di dati personali eccedenti e non pertinenti da parte di soggetti terzi (provv. 18 aprile 2013, n. 201, doc. web n. 2501014).

L'Autorità, interessata in ordine alla legittimità dell'apposizione delle generalità dell'interessato sui contrassegni forniti agli agenti di commercio per l'accesso e la sosta nella zona a traffico limitato (Ztl) cittadina, in aggiunta ad un ologramma per la lettura ottica e alla targa dell'autovettura, si è espressa sulla tipologia di dati da riportare sui predetti contrassegni nel rispetto della disciplina di riferimento (che attribuisce ai comuni la facoltà di delimitare le Ztl tenendo conto degli effetti del traffico sulla sicurezza della circolazione, sulla salute, sull'ordine pubblico, sul patrimonio ambientale e culturale e sul territorio, subordinando il transito e la sosta dei veicoli, anche al servizio delle persone disabili, a particolari condizioni ai sensi degli artt. 7, comma 9, 158, 188, 198 e 201, d.lgs. 30 aprile 1992, n. 285 (Nuovo codice della strada).

Il Garante ha quindi constatato che il comune in questione, con riferimento ai contrassegni rilasciati agli "operatori di commercio e servizi", aveva previsto l'apposizione sugli stessi della ragione sociale dell'azienda che, qualora esercitata in forma di impresa individuale, deve contenere almeno la sigla o il cognome dell'imprenditore (art. 2563 c.c.), sì da identificare direttamente l'interessato (art. 4, comma 1, lett. *b*), del Codice).

Benché tali dati debbano essere utilizzati dall'amministrazione procedente al fine di rilasciare il contrassegno per il transito e la sosta nelle Ztl, la relativa indicazione sulla parte del contrassegno esposta, leggibile da chiunque, non è risultata conforme all'art. 74, commi 1 e 2, del Codice e ha comportato una diffusione di dati personali da parte di un soggetto pubblico, operazione ammessa unicamente quando è prevista da una norma di legge o di regolamento (art. 19, comma 3, Codice). Il Garante ha pertanto prescritto al comune di non apporre in futuro sulla parte dei contrassegni che devono essere esposti sui veicoli, il nome e cognome dell'interessato eventualmente contenuti nella ragione sociale dell'azienda esercitata in forma di impresa individuale, ma di indicare solo i dati riguardanti l'autorizzazione, fissando in sei mesi il termine per adempiere (provv. 24 aprile 2013, n. 217, doc. web n. 2439150).

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

Per quanto riguarda la trasmissione di dati fra soggetti pubblici l'Autorità ha risposto a un quesito del Ministero dell'interno (Dipartimento per le libertà civili e l'immigrazione - Direzione centrale per i servizi dell'immigrazione e dell'asilo) in

merito alla comunicazione di dati personali al Garante per la protezione dell'infanzia e dell'adolescenza di una regione. La questione aveva ad oggetto la richiesta di quest'ultimo di ottenere da una prefettura della regione l'elenco nominativo dei minori accompagnati dai propri genitori presenti in un Centro di accoglienza per richiedenti asilo (Cara) e di conoscere il numero complessivo delle presenze presso il Centro, suddiviso per sesso, nonché l'elenco nominativo delle donne in gravidanza. L'Autorità ha precisato che il titolare del trattamento dei dati oggetto di richiesta è tenuto a verificare l'esistenza di una norma di legge o di regolamento che ammetta la comunicazione al Garante per la protezione dell'infanzia e dell'adolescenza dei dati personali richiesti. In mancanza di una specifica normativa, con riferimento ai soli dati diversi da quelli sensibili e giudiziari, la comunicazione è altresì ammessa quando risulti comunque necessaria per lo svolgimento di funzioni istituzionali del soggetto richiedente, sempre che le modalità della comunicazione rispettino il principio di pertinenza e non determinino presso l'amministrazione ricevente un afflusso esuberante di dati rispetto alle finalità perseguite (art. 11, comma 1, lett. *d*), del Codice). In tal caso è però necessario comunicare previamente all'Autorità tale iniziativa, evidenziando le funzioni istituzionali che il Garante per la protezione dell'infanzia e dell'adolescenza è tenuto a svolgere e per le quali sarebbe necessario ottenere i dati richiesti e verificando altresì che tali funzioni siano effettivamente realizzabili unicamente attraverso l'acquisizione dei predetti dati (artt. 19, comma 3, e 39, comma 1, lett. *a*), del Codice) (nota 23 settembre 2013).

### 4.11. *L'attività giudiziaria*

**Sicurezza nelle intercettazioni**

Nella Relazione 2012 si è riferito dell'avvio da parte del Garante degli accertamenti volti a verificare l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati personali svolti presso le Procure della Repubblica, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attività di intercettazione di conversazioni o comunicazioni, anche informatiche e telematiche, effettuate per ragioni di giustizia nonché di controllo preventivo (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.). Al fine di individuare modalità operative e di cooperazione più efficaci, l'Autorità ha inoltrato una richiesta volta ad acquisire elementi conoscitivi utili da alcune Procure della Repubblica di medie dimensioni, dislocate in diverse aree del territorio nazionale e che hanno sede presso capoluoghi di provincia.

Acquisiti tali elementi, dai quali è emerso un quadro sufficientemente ampio ed esauriente delle procedure attraverso cui detti uffici acquisiscono e gestiscono le informazioni raccolte e delle misure di sicurezza adottate da ciascuna Procura, il Garante ha rilevato l'esigenza sia di realizzare alcuni interventi volti ad assicurare un rafforzamento del livello di protezione dei dati personali trattati e dei sistemi utilizzati – commisurato alla particolare importanza e delicatezza delle informazioni detenute e alla necessaria efficacia delle indagini giudiziarie nel cui ambito le intercettazioni vengono compiute –, sia di estendere l'adozione di tali interventi alla generalità degli uffici inquirenti, anche al fine di assicurare una tendenziale omogeneità delle misure e degli accorgimenti adottati.

Il Garante ha quindi prescritto alle Procure della Repubblica misure e accorgimenti, di natura sia fisica, sia informatica, per incrementare la sicurezza dei dati personali raccolti e utilizzati nello svolgimento delle intercettazioni, anche nei casi di cd. remotizzazione degli ascolti, consistente nel reindirizzamento dei flussi delle comunicazioni dai Centri intercettazioni telecomunicazioni (C.I.T.) presso le Procure verso gli uffici di polizia giudiziaria delegata (provv. 18 luglio 2013, n. 356, doc. web n. 2551507).

**Ordine giudiziale di esibire i tabulati telefonici in una controversia civile**

Un Tribunale ha posto al Garante un quesito relativo alla legittimità del rifiuto, opposto da parte di alcune società telefoniche, di esibire in giudizio dei tabulati telefonici a fronte della richiesta congiunta delle parti interessate e dell'ordine di esibizione dell'autorità giudiziaria in sede civile, *ex* art. 210 c.p.c. Al riguardo l'Autorità ha, in primo luogo, ricordato che, trascorso il periodo di sei mesi di conservazione dei dati per finalità di fatturazione previsto dall'art. 123 del Codice, i dati relativi al traffico telefonico possono essere conservati dal fornitore per ventiquattro mesi dalla data della comunicazione per le sole finalità di accertamento e repressione di reati, potendo essere acquisiti entro tale termine con decreto motivato del pubblico ministero, mentre il difensore dell'imputato o della persona sottoposta alle indagini può acquisire i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* c.p.p. (art. 132 del Codice). Ciò premesso, l'Autorità ha richiamato il provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008 (doc. web n. 1482111), con il quale ha precisato che il vincolo secondo cui i dati conservati obbligatoriamente per legge – per l'intervallo temporale sopra precisato (profilo da riconsiderare, unitamente ad altri non meno rilevanti, alla luce della sentenza della Corte di Giustizia dell'8 aprile 2014, *Digital Rights Ireland e Seitlinger and Others*, Cause riunite C-293/12, C-594/12, aventi ad oggetto la direttiva 2006/24/CE) – possono essere utilizzati solo per finalità di accertamento e repressione di reati comporta una precisa limitazione per i fornitori nell'eventualità in cui essi ricevano richieste volte a perseguire scopi diversi, quale quello di corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile. Nella specie, quindi, il diniego opposto dalle società telefoniche alla richiesta di fornire i tabulati, ancorché d'ordine dell'autorità giudiziaria, ma in sede civile, *ex* art. 210 c.p.c., risulta legittimo. Il trattamento dei dati relativi al traffico telefonico – peraltro, limitatamente a quelli strettamente necessari a fini di fatturazione – è ammesso in sede civile solamente per controversie attinenti alla fattura telefonica.

**Trattamento di dati sensibili e giudiziari a fini di ricerca scientifica**

Un ufficio periferico del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia ha posto un quesito attinente alla legittimità della comunicazione ad una università, sulla base di un protocollo sottoscritto dalle parti e per finalità di ricerca, di dati sensibili e giudiziari di soggetti condannati ammessi all'esecuzione penale esterna. L'Autorità, premesso che, in tali casi, occorre previamente valutare se, ai fini della ricerca scientifica, non sia sufficiente il trattamento di dati anonimi, ha ricordato che il trattamento dei dati personali effettuato per scopi statistici e scientifici è regolato dagli artt. 104-110 del Codice e dalle disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (provv. 16 giugno 2004, n. 2, doc. web n. 1556635) – tra le quali assumono particolare rilievo quelle dettate dall'art. 9 – il cui rispetto costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati (art. 12 del Codice) (nota 18 aprile 2013).

**Accesso ad atti di procedura di affidamento**

Nel fornire riscontro ad una segnalante che lamentava il mancato rilascio da parte di un'assistente sociale di documenti relativi alla procedura di affidamento di sua figlia, l'Ufficio ha rilevato che la questione non rientra nella competenza del Garante (v. in argomento *supra* par. 4.3). Ove, infatti, si tratti di atti amministrativi, attesa la distinzione fra diritto di accesso ai dati personali e diritto di accesso agli atti ed ai documenti amministrativi di cui alla l. n. 241/1990, il rifiuto del destinatario a consentire l'accesso può essere oggetto di istanza di riesame avanti alla Commissione per l'accesso ai documenti amministrativi o di impugnazione avanti al competente tribunale amministrativo regionale. Ove, invece, si tratti di atti che fanno parte di un procedimento giudiziario – in quanto nella segnalazione veniva riferito che la procedura era gestita

da un tribunale per i minorenni – ogni doglianza sul comportamento dell'assistente sociale, ivi compreso il negato rilascio degli atti, deve essere sottoposta alla competente autorità giudiziaria (nota 17 ottobre 2013).

**Pubblicità dei dati nei procedimenti di espropriazione forzata**

Anche nel 2013 sono pervenute all'Autorità segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80), che prevede la pubblicazione su appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare.

**Diffusione di avvisi d'asta**

Sul tema è stato presentato un quesito con cui si è chiesto di conoscere se sia legittimo, come accaduto nel caso segnalato, che negli avvisi d'asta pubblicati nei quotidiani e nei siti internet dei vari tribunali siano contenute molteplici informazioni concernenti gli immobili posti all'asta, tenuto conto che chiunque, tramite detta pubblicità, può individuare l'interessato di cui conosca l'indirizzo di abitazione. Al riguardo, il Garante ha evidenziato che la normativa in materia di aste giudiziarie prevede, tra l'altro, la pubblicità degli avvisi d'asta, contenenti ogni informazione ritenuta utile e necessaria a descrivere gli immobili al fine del corretto espletamento della procedura di vendita, con l'omissione dell'indicazione del debitore (art. 490 c.p.c., come modificato dall'art. 174, comma 9, del Codice). Tenuto conto di ciò, con provvedimento generale del 7 febbraio 2008 (doc. web n. 1490838) il Garante ha invitato gli uffici giudiziari e i professionisti delegati alle operazioni di vendita nelle esecuzioni immobiliari ad applicare le vigenti disposizioni del codice di rito, sottolineando la necessità di omettere l'indicazione del debitore e di eventuali terzi estranei alla procedura dagli avvisi d'asta e dalla documentazione ad essi allegata. L'Ufficio ha quindi evidenziato che nell'ipotesi in cui, come nella specie, venga rispettata la prescrizione che impone di omettere l'indicazione del debitore, la pubblicità delle informazioni, anche dettagliate, concernenti gli immobili posti all'asta risulta conforme alla normativa di settore, nonché lecita sotto il profilo della disciplina in materia di protezione dei dati personali, e più specificatamente del principio di pertinenza e non eccedenza dei dati (art. 11, comma 1, lett. *d*), del Codice) (nota 5 settembre 2013).

*4.11.1. L'informatica giuridica*

**Pubblicazione di sentenze a fini di informazione giuridica**

Con riferimento alla segnalazione concernente la pubblicazione di una sentenza sul sito web di un ufficio giudiziario, recante l'indicazione in chiaro del nominativo del segnalante, l'Ufficio, nel richiamare le "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", adottate dal Garante il 2 dicembre 2010 (doc. web n. 1774813), ha ricordato che il Codice prevede all'art. 52 una specifica procedura, avviata ad istanza dell'interessato prima che sia definito il relativo grado di giudizio con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede (commi 1 - 4), per omettere i dati personali sulle sentenze e sugli altri provvedimenti giudiziari pubblicati per finalità di informazione giuridica. L'Autorità ha aggiunto che l'anonimizzazione delle pronunce è imposta dalla legge per i dati concernenti l'identità di minori oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone (comma 5). Eccettuati i suddetti casi, il Codice ammette la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali (comma 7) (nota 7 ottobre 2013).

Il Garante per l'infanzia e l'adolescenza di una regione e l'Associazione nazionale famiglie adottive e affidatarie hanno segnalato che in una rivista di informazione giuridica era stata pubblicata *online* una sentenza di un Tribunale per i minorenni emessa in un procedimento in materia di adottabilità di una minore, in versione

integrale, ovvero recante in chiaro il nominativo della minore e altri dati idonei ad identificarla, ivi compresi il luogo e la data di nascita e il nome della madre. L'Autorità, nel chiedere al gestore della rivista l'immediata anonimizzazione della sentenza, mediante l'omissione di ogni dato dal quale poteva desumersi, anche indirettamente, l'identità della minore nonché della madre, della quale veniva riportato l'episodio di una violenza sessuale, ha ricordato i divieti di diffondere dati da cui possa desumersi anche indirettamente l'identità di minori (art. 52, comma 5, del Codice) e le generalità delle persone offese (tra l'altro) da atti di violenza sessuale senza il loro consenso (art. 734-*bis* c.p., richiamato anche dal citato comma 5 dell'art. 52) (nota 5 settembre 2013).

Con successiva nota l'Autorità ha preso atto della espunzione della sentenza dal sito della rivista, ricordando altresì che l'anonimizzazione deve essere curata anche con riferimento alle eventuali massime estratte dai provvedimenti giurisdizionali, che non devono contenere informazioni dalle quali sia possibile risalire all'identità dei soggetti tutelati (nota 17 settembre 2013).

*4.11.2. Le notificazioni di atti e comunicazioni*

Nel 2013 sono pervenute diverse segnalazioni circa le modalità di notificazione di atti giudiziari in modo non conforme alle prescrizioni del Codice.

**Notificazioni di atti giudiziari a mezzo posta**

In una segnalazione si è lamentato che sulla busta di notificazione di un atto giudiziario destinato al segnalante e proveniente da uno studio legale, era stata apposta la dicitura "a mani proprie perché è una separazione x il portalettere".

L'Ufficio notifiche della Corte d'appello competente ha rappresentato che era consuetudine dell'ufficio, per la mole di lavoro e la carenza di personale, ricevere atti per la notificazione a mezzo del servizio postale già completi di busta e cartolina verde precompilati dai richiedenti e che, nella specie, la busta era stata già compilata con tutte le diciture a cura di un ufficio legale. Al riguardo l'Ufficio ha evidenziato che la normativa di settore in tema di notifiche di atti giudiziari affida all'ufficiale giudiziario, se non è disposto altrimenti, il compito di eseguire le notificazioni (art. 137 c.p.c.) e, quando queste vengono effettuate a mezzo posta, gli ufficiali giudiziari devono fare uso di speciali buste sulle quali non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto (art. 2, l. n. 890/1982, come modificato dall'art. 174 del Codice). Si è pertanto ritenuto che l'ordinamento giuridico affida all'ufficiale giudiziario il compito e la responsabilità, anche al fine del risarcimento dell'eventuale danno provocato dal non corretto trattamento dei dati, di curare gli adempimenti relativi alla notificazione di atti giudiziari, e che non assume rilievo la circostanza che l'indirizzamento sulla busta sia predisposto da altri (nota 16 gennaio 2013).

**Notificazioni di atti giudiziari presso il luogo di lavoro**

Un cittadino ha segnalato di avere ricevuto, nell'ambito di alcuni procedimenti penali che lo vedono coinvolto a vario titolo, notifiche di atti giudiziari da parte di una Procura della Repubblica presso il luogo di lavoro, anziché al domicilio eletto presso il proprio difensore, con la conseguenza della conoscenza del contenuto degli atti da parte di un numero di soggetti maggiore di quelli che sarebbero stati coinvolti nel caso in cui la notifica fosse stata effettuata presso il domicilio eletto. Effettuate le necessarie verifiche, l'Autorità ha rilevato che anche i trattamenti effettuati per ragioni di giustizia debbono rispettare il principio posto dall'art. 11 del Codice relativo alla non eccedenza del trattamento rispetto alle finalità per le quali i dati personali sono raccolti o successivamente trattati. La disciplina legale delle forme di notifica di atti giudiziari, come pure modificata dal Codice (art. 174), garantisce la tutela della riservatezza dei dati personali, unitamente all'esigenza di assicurare lo svolgimento delle funzioni giudiziarie. Poiché nella vicenda risultava che, in un caso, la