11. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Le operazioni di trasferimento dei dati personali all'estero sono state oggetto di particolare attenzione nel corso di tutto il 2009, sia con riferimento allo strumento delle *Binding corporate rules* (*Bcr*) (Norme vincolanti d'impresa), sia relativamente alla materia delle *Standard contractual clauses* (Clausole contrattuali tipo).

Il lavoro di approfondimento condotto dal Gruppo Art. 29, in relazione alle modalità e ai tempi di approvazione delle *Binding corporate rules*, ha prodotto positivi risultati in materia di accelerazione dei termini di definizione delle procedure di cooperazione europea e di proficua partecipazione delle autorità di protezione dei dati alla definizione dei testi da sottoporre ad autorizzazione nazionale. In più casi è stato interessato il Garante che, nel pronunciarsi favorevolmente in ordine ai progetti di *Bcr* elaborati da diversi gruppi societari di carattere multinazionale, si è dichiarato disponibile all'instaurazione della procedura nazionale volta al rilascio della relativa autorizzazione.

Molte delle procedure appena menzionate sono state condotte nell'ambito dell'accordo di mutua collaborazione assunto da 18 autorità (tra cui il Garante italiano) con l'obiettivo di accelerarne i tempi di conclusione e di semplificare l'attività di revisione degli schemi di *Bcr* predisposti dalle società.

Particolarmente intensa è stata, inoltre, l'attività di riflessione condotta in materia di *Standard contractual clauses* con riferimento alla proposta della Commissione europea volta all'adozione di un nuovo *set* di clausole da titolare a responsabile. In merito, diversi sono stati i contributi forniti da questa Autorità nell'ambito delle attività di approfondimento condotte dal Gruppo Art. 29 e relativamente alla redazione del parere in materia (*Opinion WP 161*).

Analoga attenzione è stata dedicata all'analisi della decisione della Commissione di recente approvazione (n. 2010/87/EU del 5 febbraio 2010) che, nel dar corso alla proposta succitata, sostituisce il *set* di clausole contrattuali tipo da titolare a responsabile, già esistente (decisione della Commissione n. 2002/16/EC), con un nuovo schema il quale, nel tentativo di meglio rappresentare la complessa realtà dell'affidamento

in *outsourcing*, prevede al proprio interno una clausola, *cd. "di subcontracting"* secondo la quale l'importatore (in qualità di responsabile del trattamento) può affidare il trattamento (o una parte di esso) a un soggetto terzo (*cd. "subcontractor"*), che agisce anch'esso come responsabile. E' tuttora in corso di definizione l'attuazione, con autorizzazione del Garante, della decisione medesima.

12. LIBERE PROFESSIONI

12.1. ORDINI PROFESSIONALI

Nel corso del 2009 l'Autorità ha fornito alcuni chiarimenti a professionisti circa le modalità con le quali gli ordini o i collegi professionali possono legittimamente trattare i dati personali dei propri iscritti.

In particolare, un ingegnere aveva ipotizzato una presunta violazione del Codice per la mancata pubblicazione, nell'albo, dei numeri di telefono, di fax e degli indirizzi di posta elettronica di alcuni colleghi. Dall'esame della normativa di settore è risultato che nell'albo degli ingegneri devono essere inseriti, per ogni singolo iscritto, il nome, il cognome e la residenza, che per i cittadini dell'Unione europea è parificata al domicilio professionale ai fini dell'iscrizione o del mantenimento in albi (*cfr.* art. 3, r.d. 23 ottobre 1925, n. 2537, art. 16, l. 21 dicembre 1999, n. 526).

Inoltre, il Codice prevede che gli ordini e collegi professionali possono, a richiesta della persona iscritta all'albo che vi abbia interesse, inserire nei rispettivi albi dati ulteriori rispetto a quelli previsti dalla normativa di settore, pertinenti e non eccedenti, in relazione all'attività professionale (*cfr.* art. 61, comma 3, del Codice).

Su tali basi l'Ufficio ha ritenuto che la mancata pubblicazione sull'albo degli ingegneri di informazioni ulteriori rispetto a quelle previste dalla normativa di settore non violasse il Codice (*Nota* 11 novembre 2009).

Il Consiglio nazionale del notariato (Cnn) aveva manifestato al Garante l'intenzione di realizzare un sistema centralizzato di archiviazione dei dati personali riportati nei repertori ed archivi degli studi notarili e di utilizzare tali dati, in forma anonima, per finalità statistiche, conferendo la gestione del sistema alla società che realizza e cura i servizi informatici e telematici per i notai italiani.

Per garantire il pieno rispetto della normativa, l'Autorità ha evidenziato che il predetto sistema di archiviazione può essere realizzato sempreché ogni singolo notaio, che decida di aderire all'iniziativa, designi la società Notartel quale responsabile del trattamento dei suddetti dati (art. 29 del Codice). È stata, inoltre, richiamata l'attenzione sul rispetto

degli obblighi di sicurezza e delle misure minime indicate nelle regole tecniche di cui all'Allegato B. al Codice (artt. 31, 33 *ss.* del Codice).

In merito al trattamento dei suddetti dati per finalità statistiche, l'Autorità ha evidenziato la necessità che presso il Cnn si proceda preventivamente alla costituzione dell'ufficio di statistica, nel rispetto del quadro normativo di settore, anche con riferimento all'informativa da rendere agli interessati (*cfr.* d.lgs. 6 settembre 1989, n. 322); infatti le informazioni in questione si qualificano come dati personali, ancorché non direttamente identificativi, a norma del Codice e del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (art. 4, comma 1, lett. *c*) e Allegato A.3. al Codice [doc. *web* n. 43293]) (*Nota* 21 ottobre 2009).

12.2. ATTIVITÀ FORENSE

Anche nel 2009 si è registrato un incremento dell'attività legata alle segnalazioni e ai reclami relativi all'attività forense, con particolare riferimento al trattamento di dati personali anche sensibili effettuato dagli avvocati nell'ambito di procedimenti giudiziari civili e penali.

Produzione di documenti in giudizio

In merito alla produzione di documenti di varia natura in sede giudiziaria, l'Autorità ha ribadito che ogni valutazione in ordine alla validità, efficacia e utilizzabilità in giudizio di atti, documenti e provvedimenti basati sul trattamento di dati personali, anche ove il trattamento medesimo non sia conforme alle disposizioni di legge o di regolamento, spetta, ai sensi dell'art. 160, comma 6, del Codice, al giudice e non al Garante (*Note* 27 ottobre 2009, 5 novembre 2009 e 16 ottobre 2009).

Visione e copia di atti processuali

Nel caso di presa visione ed estrazione di copia di atti contenuti nei fascicoli processuali, l'Autorità ha ricordato che il Codice (art. 51) non ha modificato le norme concernenti la visione ed il rilascio di estratti e di copie di atti e documenti, contenute nei codici di procedura civile e penale (*Nota* 22 ottobre 2009).

Il consenso degli interessati

Alcune segnalazioni hanno riguardato il trattamento di dati personali in sede giudiziaria da parte di avvocati senza il consenso degli interessati. In tali occasioni l'Autorità ha

rappresentato che, ai sensi dell'art. 24, comma 1, lett. *f*), del Codice, il consenso non è richiesto quando il trattamento è necessario *"per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento"*. Ha inoltre precisato che, in tali ipotesi, non è richiesta l'informativa all'interessato, ove i suoi dati personali siano raccolti presso terzi (art. 13, comma 5, lett. *b*), del Codice) (*Note* 16 ottobre 2009, 5 novembre 2009 e 20 ottobre 2009).

Conservazione dei dati

E' stato affrontato il tema dei limiti temporali della conservazione, da parte degli avvocati, di dati personali, anche sensibili, successivamente alla conclusione del processo al quale afferiscono.

A tale proposito, il Garante ha ricordato (*Nota* 5 novembre 2009) che il codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria ([doc. *web* n. 1565171], *v. Relazione 2008*, p. 166) stabilisce, al riguardo (art. 4), che la definizione di un grado di giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati da parte del difensore.

Una volta estinto il procedimento o il relativo rapporto di mandato, atti e documenti attinenti all'oggetto della difesa o delle investigazioni difensive possono essere conservati, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento.

Con specifico riferimento ai dati sensibili, inoltre, l'Autorità ha ricordato (*Nota* 5 novembre 2009) che l'*autorizzazione* n. 4/2008 al trattamento dei dati sensibili da parte dei liberi professionisti [doc. *web* n. 1529408] prevede al punto 5) che i dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

Alcune segnalazioni hanno riguardato anche il trattamento dei dati personali svolto da investigatori privati.

In particolare, in un caso è stata posta la questione del mandato a svolgere attività investigative in sede di indagini preliminari rilasciata, ad un investigatore privato, dalla parte

personalmente, benché l'art. 327-*bis* c.p.p., in tema di attività investigative svolte nel corso di indagini preliminari, preveda, al comma 3, che tali attività possano essere svolte da investigatori privati autorizzati su incarico del difensore.

Nell'occasione l'Autorità ha osservato (*Nota* 27 ottobre 2009) che - ferma ogni eventuale conseguenza sul piano processuale che non spetta al Garante valutare, e con esclusivo riferimento agli aspetti riguardanti la protezione dei dati personali - il codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive, nel disciplinare anche i trattamenti da parte di investigatori privati, stabilisce che questi possono svolgere le loro attività solo sulla base di uno specifico mandato scritto, che può essere rilasciato sia da un legale, sia da altro soggetto (art. 8, commi 2 e 6).

A seguito di alcune segnalazioni, l'Autorità ha, inoltre, accertato il rispetto del menzionato codice deontologico da parte di alcune agenzie investigative, con particolare riferimento al rispetto degli obblighi di non divulgare a terzi le informazioni raccolte e dell'effettiva consegna ai committenti, al termine delle indagini, di tutta la documentazione raccolta (*Nota* 9 febbraio 2010).

13. TRATTAMENTO DEI DATI PERSONALI IN AMBITO CONDOMINIALE

Alcuni condòmini avevano lamentato l'illecita affissione in spazi accessibili al pubblico, da parte dell'amministratore del condominio, di un avviso di rimozione delle loro autovetture parcheggiate nel cortile condominiale (oggetto di lavori per la costruzione di posti auto interrati), indicante il numero di posto auto, le targhe dei veicoli, nonché le foto delle auto medesime. Gli stessi segnalanti avevano inoltre contestato l'indebita comunicazione a terzi (il legale di fiducia dello stesso condominio e soggetti incaricati, a vario titolo, dei lavori) dell'inosservanza di una delibera assembleare e della targa della relativa autovettura.

L'Autorità (*Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]) rilevato che, nel caso di specie, si sarebbero potute adottare modalità parimenti efficaci ma meno invasive per gli interessati, ha ritenuto la predetta affissione contraria ai princìpi di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), prescrivendo al condominio di rivolgersi singolarmente ai partecipanti alla compagine condominiale. Parimenti illecita e sproporzionata è risultata la comunicazione ai soggetti a vario titolo coinvolti nell'appalto dei dati personali riferiti agli interessati; ciò tenuto conto che la mancata rimozione degli autoveicoli riconducibili ai segnalanti risultava già comprovata dal materiale fotografico prodotto in atti e che la presenza *in loco* delle stesse imprese appaltatrici (impossibilitate all'esecuzione dei lavori deliberati proprio in ragione della presenza dei veicoli non rimossi) non giustifica tale comunicazione.

È stata dunque vietata al condominio l'ulteriore comunicazione ai soggetti sopra menzionati dei dati riferiti ai segnalanti, ma è stata ritenuta lecita la comunicazione dei predetti dati al legale, considerata la necessità manifestata dal condominio di doversi tutelare in sede giudiziaria (art. 24, comma 1, lett. *f*), del Codice).

Il Garante si è occupato (anche) delle modalità di presentazione della denuncia relativa al calcolo e al versamento della tassa per lo smaltimento dei rifiuti solidi urbani (*cd.* "Tarsu").

In particolare, il *provvedimento* 19 febbraio 2009 [doc. *web* n. 1601650]

ha ad oggetto la comunicazione dei dati personali riferiti ad un condòmino da parte dell'amministratore, nell'ambito della procedura di trasmissione al comune competente, dei dati utili al calcolo della tassa menzionata.

Il conduttore di un immobile, con reclamo, aveva lamentato il deposito, da parte dell'amministratore del condominio, della denuncia di *"occupazione o detenzione di locali o aree"* ai fini del versamento della Tarsu, relativa alla sua posizione tributaria. Benché avesse già assolto tale obbligo di denuncia e diffidato l'amministratore dal provvedervi, per effetto della dichiarazione inoltrata, a sua insaputa, dall'amministratore stesso, il reclamante avrebbe ricevuto la notifica di due avvisi di pagamento riferiti allo stesso periodo di occupazione per il medesimo immobile.

Il regolamento comunale, in assenza della trasmissione dei dati da parte dei soggetti tenuti alla dichiarazione, per tali posizioni residue poneva in capo agli enti proprietari, agli enti gestori o agli amministratori di condominio la responsabilità del versamento di quanto dovuto (art. 27, comma 3, regolamento *cit.*).

Con il citato *provvedimento* il Garante, nel ritenere il trattamento lecito in astratto (art. 24, comma 1, lett. *a*), del Codice) ha tuttavia ritenuto che la comunicazione nei confronti degli uffici comunali fosse avvenuta in violazione del principio di correttezza (art. 11, comma 1, lett. *a*), del Codice).

Infatti l'amministratore, per evitare la consegna di dichiarazioni diverse riferite allo stesso contribuente e al contempo prevenire l'insorgere di una possibile responsabilità a proprio carico avrebbe dovuto, prima della comunicazione dei dati del reclamante, accertarsi presso gli uffici comunali competenti dell'effettivo mancato adempimento dell'obbligo gravante sul soggetto passivo della tassa.

Pertanto l'Autorità ha prescritto, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, all'amministratore condominiale di porre in essere ogni previa scrupolosa verifica dell'avvenuta presentazione della stessa da parte degli occupanti dello stabile amministrato al fine di prevenire denunce ripetute o inesatte.

14. SICUREZZA DEI DATI E DEI SISTEMI

14.1. CONSERVAZIONE DEI DATI DI TRAFFICO: MISURE E ACCORGIMENTI A GARANZIA DEI CITTADINI

Anche nel 2009, il Garante si è occupato di questioni legate al tema della conservazione dei dati di traffico telefonico e telematico sia per finalità di accertamento e repressione dei reati sia per altre finalità ordinarie.

In primo luogo, il Garante è nuovamente intervenuto in relazione ai termini entro i quali i fornitori di servizi telefonici e telematici sono tenuti a conformare i propri sistemi alle misure e agli accorgimenti prescritti con il *provvedimento* 17 gennaio 2008 [doc. *web* n. 1482111] come integrato il 24 luglio 2008 [doc. *web* n. 1538224], dei quali si è dato atto nella *Relazione 2008*, p. 173.

Infatti, nel mese di aprile 2009 numerose richieste di associazioni rappresentative del settore delle comunicazioni elettroniche hanno rappresentato una situazione di sostanziale, ma non ancora integrale, adeguamento, per la quasi totalità dei fornitori, alle prescrizioni contenute nel suindicato provvedimento, con particolare riferimento alle misure e agli accorgimenti prescritti alla lettera *a*), nn. 3, 6 e 9 e alla lettera *c*) dello stesso.

Le medesime associazioni hanno, quindi, richiesto al Garante una proroga dei termini indicati nel citato *provvedimento* del 24 luglio 2008, al fine di completare l'attuazione delle richiamate prescrizioni, rispetto alle quali peraltro i fornitori hanno dichiarato di aver già raggiunto un elevato livello di adeguamento.

L'Autorità in ragione dell'elevato numero di piattaforme e sistemi aziendali coinvolti negli adempimenti previsti dal provvedimento, dell'altrettanto elevato numero di processi aziendali da essi supportati e, quindi, della complessità degli interventi necessari per l'adeguamento degli stessi, nonché della mole degli investimenti complessivi previsti e di quelli già impegnati ha accordato la richiesta proroga, anche se limitatamente ad alcune misure specificamente indicate. Pertanto, con il *provvedimento* 29 aprile 2009 (in *G.U.* 11 maggio 2009, n. 107 [doc. *web* n. 1612508]), è stato individuato il nuovo termine nel 15 dicembre 2009, prevedendo altresì che, entro la medesima data, tutti i titolari del

trattamento interessati dovessero dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento.

Nel corso dell'anno, inoltre, l'Autorità ha svolto una verifica sul rispetto della normativa in materia di *data retention* da parte dei fornitori di servizi telefonici e telematici che operano in Italia.

La menzionata attività va ricondotta anche alla decisione del Gruppo Art. 29 di disporre un'azione di *enforcement* volta a verificare l'osservanza, da parte dei fornitori di servizi di comunicazione elettronica, degli obblighi fissati nella normativa nazionale in materia di *data retention*, sul fondamento degli artt. 6 e 9 della Direttiva n. 2002/58/CE e della Direttiva n. 2006/24/CE.

La complessa attività istruttoria ha riguardato servizi telefonici e telematici - individuati, in primo luogo, tra quelli che non erano stati oggetto degli accertamenti svolti dall'Autorità sin dal 2005 e dei provvedimenti adottati nel corso dell'anno 2008 - sulla base di alcuni criteri ai quali aveva fatto riferimento anche il Gruppo Art. 29 (*ad es.*, il fatto di essere operatori telefonici "virtuali" ovvero fornitori di servizi esclusivamente telematici).

In particolare, è stato consegnato ai quattro fornitori coinvolti nell'accertamento, unitamente a richieste di informazioni ai sensi dell'art. 157 del Codice sull'attuazione degli adempimenti sopra indicati, un questionario appositamente predisposto nell'ambito dell'*enforcement.*

In base alle risposte pervenute, l'Autorità ha proceduto nei mesi di settembre e ottobre con gli accertamenti ispettivi presso le sedi delle società, concentrandosi essenzialmente sulle criticità emerse rispetto alla disciplina della *data retention*, risultate peraltro, nella maggior parte dei casi, di facile risoluzione tecnica.

L'Autorità in ragione delle violazioni accertate - tempi di conservazione dei dati di traffico telefonico e telematico superiori al consentito; conservazione di informazioni sui siti visitati dagli utenti - ha successivamente adottato tre *provvedimenti* (21 ottobre 2009 [doc. *web* n. 1683093] e 19 novembre 2009 [doc. *web* nn. 1695393 e 1695368]) nei confronti di altrettante società tra quelle coinvolte nell'istruttoria, disponendo in due casi

anche la trasmissione degli atti alla magistratura per la valutazione di eventuali profili penali.

Al riguardo l'Autorità ha innanzitutto prescritto la cancellazione dei dati di traffico telefonico e telematico conservati oltre i tempi previsti dalla normativa a fini di accertamento e repressione dei reati (12 mesi per i dati di traffico telematico e 24 mesi per quelli di traffico telefonico).

Ha inoltre prescritto di cancellare tutte le informazioni in grado di rivelare gusti, opinioni, tendenze degli utenti che non avrebbero mai dovuto essere archiviate nei *database* (*ad es.*, l'oggetto dei messaggi di posta elettronica inviati e ricevuti; i dati personali relativi alla navigazione in internet, anche quando rappresentati dal solo indirizzo *Ip* di destinazione).

Ad una società è stato prescritto, al fine di innalzare i livelli di sicurezza dei flussi informativi con l'autorità giudiziaria e di garantire in modo più adeguato la riservatezza delle informazioni, di sostituire il fax con sistemi di comunicazione sviluppati con protocolli di rete sicuri e strumenti di cifratura basati su firma digitale.

14.2. IL RUOLO DEGLI AMMINISTRATORI DI SISTEMA NELLA SICUREZZA DEI TRATTAMENTI

Come indicato nella *Relazione 2008* (p. 178 *ss.*), il ruolo dell'amministratore di sistema e la rilevanza strategica di questa figura nell'ambito della protezione dati sono stati oggetto di interesse da parte dell'Autorità che, con *provvedimento* 27 novembre 2008 (*G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]), aveva richiamato tutti i titolari di trattamenti effettuati, anche solo in parte, mediante strumenti elettronici, alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, individuando altresì le misure da adottare per agevolare la verifica sull'attività degli amministratori da parte dei titolari delle banche dati e dei sistemi informatici.

In ragione della complessità degli interventi organizzativi e tecnici a tali fini necessari e delle richieste pervenute da numerosi soggetti pubblici e privati, il Garante ha

successivamente avviato una consultazione pubblica (*Provv.* 21 aprile 2009, in *G.U.* 8 maggio 2009, n. 105 [doc. *web* n. 1611986]) volta ad acquisire osservazioni ed opinioni tecniche da parte dei titolari del trattamento ai quali il provvedimento originale era rivolto. La consultazione, durata poco più di un mese, ha coinvolto numerosi soggetti pubblici, le principali aziende del settore dell'*information technology*, nonché alcune importanti associazioni di categoria, mettendo in luce la complessità tecnica di attuazione del provvedimento riscontrata in alcune realtà pubbliche e private di grandi dimensioni.

La consultazione ha inoltre ha fatto emergere importanti considerazioni relative ai trattamenti effettuati mediante l'uso di servizi in *outsourcing* e di terze parti in qualità di amministratori di sistema.

Pertanto, in ragione dei contributi pervenuti e delle considerazioni maturate nell'ambito della consultazione pubblica, l'Autorità ha differito al 15 dicembre 2009 i termini di adeguamento al provvedimento (*Provv.* 25 giugno 2009, in *G.U.* 30 giugno 2009, n. 149 [doc. *web* n. 1626595]), introducendo anche alcune modifiche al testo originale, per semplificare l'implementazione delle misure previste nei casi di trattamenti effettuati in *outsourcing* o mediante subappalti della gestione dei sistemi informativi.

15. LA VIDEOSORVEGLIANZA E LA BIOMETRIA

15.1. VIDEOSORVEGLIANZA IN AMBITO PUBBLICO

L'attività nel periodo considerato ha riguardato l'applicazione del *provvedimento* generale in materia di videosorveglianza del 2004 ([doc. *web* n. 1003482], *cfr. Relazione 2004*) e, in seguito a consultazioni di carattere istituzionale con l'Anci (Associazione nazionale comuni italiani) ed il Ministero dell'interno, l'adozione del nuovo *provvedimento* in materia (8 aprile 2010 [doc. *web* n. 1712680]).

Per quanto riguarda il *provvedimento* del 2004 l'Autorità, nel rispondere a molteplici segnalazioni e quesiti, ha fornito ulteriori indicazioni sulla sua corretta applicazione.

Numerosi comuni hanno adottato uno specifico regolamento disciplinante le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio, che hanno successivamente trasmesso al Garante per ottenerne l'approvazione ovvero solo per porre a conoscenza l'Autorità di tale iniziative. Al riguardo, è stato rappresentato che l'installazione di tali sistemi non deve essere sottoposta all'esame preventivo dell'Autorità. In particolare, non può desumersi alcuna approvazione implicita dal silenzio del Garante dopo la ricezione di regolamenti, progetti o comunicazioni relativi all'intenzione di installare tali sistemi (*cfr.* punto 3.2., *Provv. cit.*) (*Note* 13 novembre 2009, 20 novembre 2009 e 13 gennaio 2010).

Ad uno dei comuni che aveva trasmesso il proprio regolamento l'Ufficio ha, altresì, precisato che le iniziative di videosorveglianza devono essere precedute da una corretta valutazione, alla luce dei princìpi di liceità, necessità, pertinenza, non eccedenza e proporzionalità rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice). Pertanto, non risulta lecito procedere ad una videosorveglianza capillare di intere aree cittadine "cablate", riprese integralmente, costantemente e senza adeguate esigenze (*cfr.* punto 5.1., *Provv. cit.*) (*Nota* 20 luglio 2009).

Un comune aveva manifestato l'intenzione di montare stabilmente telecamere, per sole riprese video, a bordo di veicoli utilizzati dalla polizia locale, ma privi di contrassegni identificativi dell'ente di appartenenza, con la finalità specifica di contrastare il fenomeno

dell'abbandono dei rifiuti sul territorio di competenza. Al riguardo, è stato precisato che non sono previste, da parte del Garante, ipotesi di autorizzazione per esentare dall'obbligo di fornire l'informativa agli interessati nell'ambito di un trattamento di dati personali effettuato tramite sistemi di videosorveglianza (art. 13 del Codice). Nel citato *provvedimento* è specificato che coloro i quali transitano nelle aree sorvegliate devono essere informati della rilevazione dei dati. L'informativa deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi (*cfr.* punto 3.1. *Provv. cit.*) (*Nota* 13 gennaio 2010).

Si è fatto più volte presente che resta, tuttavia, ferma l'esenzione, prevista dalla legge, dall'obbligo di fornire l'informativa agli interessati in relazione alle ipotesi di trattamento di dati personali effettuato *"da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento e repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento"* (art. 53 del Codice) (*Note* 9 dicembre 2009 e 13 gennaio 2010).

Infine, l'Autorità è stata chiamata, in più occasioni, a pronunciarsi sui tempi di conservazione delle immagini raccolte tramite sistemi di videosorveglianza.

In particolare, Sogei S.p.A. (società di *information and communication technology* del Ministero dell'economia e delle finanze), che gestisce i dati, anche sensibili, di tutti i contribuenti e di tanti altri cittadini, aveva chiesto di essere autorizzata a conservare le immagini raccolte oltre le ventiquattro ore, così come previsto dal *provvedimento* del 2004 (*cfr.* punto 3.4., *Provv. cit.*), e per un periodo massimo di sette giorni. Con riferimento ai tempi di conservazione, il Garante ha stabilito che va comunque applicato il principio di proporzionalità e che, quindi, l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere le finalità perseguite (art. 11, comma 1, lett. *d*) ed *e*) del Codice).

In tale quadro, vista la particolare rischiosità dell'attività che svolge la Sogei per la natura dei dati trattati, l'Ufficio ha ritenuto proporzionato che la stessa conservi le immagini raccolte tramite sistemi di videosorveglianza per un periodo di tempo non superiore alla settimana (*Nota* 11 novembre 2009).

L'Autorità si è espressa nei medesimi termini nei confronti della Soprintendenza per i beni storici, artistici e etnoantropologici per le province di Bo, Fe, Fc, Ra, e Rn, che aveva chiesto, per le immagini raccolte presso la Pinacoteca Nazionale di Bologna, la conservazione per un tempo superiore alle ventiquattro ore e non eccedente le settimana (*Nota* 10 febbraio 2010).

Da ultimo, si menziona la vicenda relativa alla Soprintendenza speciale per il polo museale napoletano che si era rivolta all'Autorità dopo aver ricevuto dal Comando dei Carabinieri-tutela patrimonio culturale nucleo di Napoli la richiesta di conservare le immagini raccolte tramite i sistemi di videosorveglianza, installati presso alcuni siti museali della Regione Campania, per un periodo di almeno trenta giorni, al fine di tutelare, nell'ambito del progetto *"Allarme sicurezza musei"*, i siti d'interesse culturale che potrebbero essere maggiormente esposti al rischio della minaccia terroristica. Dall'esame della normativa di settore è emerso che è possibile effettuare controlli continuativi tramite impianti audiovisivi per garantire la sicurezza dei beni culturali raccolti nei musei statali (art. 1, d.l. 14 novembre 1992, n. 433).

Il Garante ha precisato che, anche nelle ipotesi in cui specifiche disposizioni di legge consentano l'installazione di telecamere in tema di sicurezza, è comunque necessario - qualora siano trattati dati relativi a persone identificate o identificabili - rispettare i princìpi generali di liceità, necessità, proporzionalità e finalità affermati dal Codice (artt. 3, 11, comma 1, lett. *a*) e *d*) e 18, comma 2, del Codice e punto 2.1., *Provv. cit.*).

Inoltre, ha ribadito che, in base al principio di proporzionalità, l'eventuale allungamento, oltre una settimana, dei tempi di conservazione di tali dati deve essere valutato come eccezionale e relativo a specifiche necessità derivanti da eventi già accaduti o realmente incombenti, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso (*cfr.* punto 3.4., *Provv. cit.*). Alla luce delle considerazioni sopra richiamate, il Garante ha prescritto alla Soprintendenza speciale per il polo museale napoletano, con *provvedimento* adottato ai sensi dell'articolo 154, comma 1, lett. *c*) del Codice, di conservare le immagini raccolte presso alcuni siti museali della Regione Campania

per un periodo di trenta giorni, finché persiste la dichiarata eccezionale necessità (*Provv.* 12 marzo 2009 [doc. *web n.* 1605521]).

In ordine ai sistemi di videosorveglianza, è da rilevare l'approvazione (condizionata) di un apparato di videosorveglianza presso un istituto scolastico di Verona, sottoposto a verifica preliminare dell'Autorità, nell'ambito di un progetto più ampio denominato *"Scuole sicure"*, a fini di prevenzione e deterrenza contro teppismo ed atti vandalici, a salvaguardia del patrimonio scolastico.

Il Garante ha approvato tale progetto, con taluni limiti, a tutela di ragazzi, docenti e personale scolastico. E' stata disposta infatti, in conformità al *provvedimento* generale sulla videosorveglianza del 29 aprile 2004, l'entrata in funzione delle telecamere solo negli orari di chiusura degli istituti; in caso di attività all'interno della scuola che potrebbero iniziare e concludersi in coincidenza con l'orario di attivazione delle telecamere è stata prevista l'esigenza di definire, in accordo con il dirigente scolastico, gli orari di funzionamento delle telecamere.

Le telecamere possono riprendere esclusivamente le mura esterne, devono essere segnalate da appositi cartelli con visibilità anche notturna e la visualizzazione delle immagini è stata consentita solo a polizia e autorità giudiziaria (*Provv.* 4 settembre 2009 [doc. *web* n. 1651744]).

Il nuovo provvedimento in materia di videosorveglianza

Il nuovo *provvedimento* generale in materia di videosorveglianza [doc. *web* n. 1712680], che sostituisce quello del 29 aprile 2004 [doc. *web* n. 1003482], adottato visto lo sviluppo della tecnologia, i numerosi interventi normativi, statali e regionali - che hanno incentivato l'utilizzo della videosorveglianza come forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici, nonché le molteplici finalità per le quali tali sistemi sono utilizzati - delinea un nuovo quadro di garanzie a tutela degli interessati fornendo, contestualmente, specifiche prescrizioni ai titolari del trattamento.

In considerazione della rilevanza della tematica, se ne dà conto di seguito in dettaglio.

Preliminarmente sono stati consultati il Ministero dell'interno, l'Associazione nazionale comuni italiani (Anci) e l'Unione delle province d'Italia (Upi), affinché ciascuno, per i propri profili di competenza, formulasse le proprie osservazioni.