# 13 Concessionari di pubblici servizi

L'attività dell'Autorità in continuità con le azioni intraprese nel 2006, si è concentrata, in particolare, su due filoni di intervento: le *cd. "dichiarazioni stragiudiziali"* e le modalità di trattamento di dati poste in essere dall'Agenzia delle entrate (in qualità di titolare del trattamento) e dalla Rai-Radiotelevisione italiana (quale responsabile del trattamento), mediante il ricorso ad "agenti" privati (comunemente noti come "ispettori Rai") per contrastare il fenomeno del mancato pagamento del canone per i servizi radiotelevisivi.

**Dichiarazioni stragiudiziali**

Sono giunte diverse segnalazioni sulle *"dichiarazioni stragiudiziali"* che il concessionario del servizio per la riscossione dei tributi può chiedere (ai sensi dell'art. 75-*bis* del d.P.R. n. 602/1973, come modificato dalla legge n. 211/2004, recante la legge finanziaria per il 2005, art. 1, comma 425) anche prima di procedere al pignoramento presso terzi, ai debitori del soggetto iscritto a ruolo, per conoscere le cose e le somme da essi dovute al soggetto medesimo.

In relazione a tale normativa, dalla formulazione piuttosto generica, il Garante aveva previsto l'obbligo dei concessionari suddetti di informare preventivamente il soggetto iscritto a ruolo circa la possibilità, in caso di mancato pagamento, dell'acquisizione presso terzi della dichiarazione medesima (*cfr. Provv.* 25 maggio 2005, [doc. *web* n. 1131826] e *Relazione* 2006, *p.* 115).

A seguito dell'adozione del *provvedimento*, sono pervenute numerose segnalazioni, da parte di cittadini, concernenti prevalentemente violazioni dell'obbligo di rilascio della previa informativa.

Successivamente, la legge n. 286/2006 ha riscritto l'art. 75-*bis* del d.P.R. n. 602/73, stabilendo espressamente che gli agenti della riscossione possono procedere al trattamento dei dati personali acquisiti tramite dichiarazione stragiudiziale senza rendere l'informativa prevista all'art. 13 del Codice in materia di protezione dei dati personali.

L'attività del Garante, in parte ancora in corso, ha tenuto conto di tale ulteriore modifica del quadro normativo e ha peraltro rilevato, in diverse occasioni, il mancato rispetto dei princìpi di pertinenza e di non eccedenza nei trattamenti posti in essere dagli agenti della riscossione.

**Agenzia delle entrate e Rai-Radiotelevisione italiana S.p.A.**

Il Garante ha definito con *provvedimento* del 5 marzo 2008 [doc. *web* n. 1501024] l'istruttoria condotta nel 2007 sul trattamento di dati personali effettuato dall'Agenzia delle entrate-Sportello abbonamenti TV e presso Rai-Radiotelevisione italiana S.p.A. per finalità di promozione e di recupero del canone radiotelevisivo.

Numerose segnalazioni avevano lamentato comportamenti irrituali da parte di "ispettori" Rai, con toni minacciosi e modalità ritenute "inquisitorie" e "intimidatorie" nella raccolta di dati personali, anche in relazione alla prospettazione di possibili accertamenti intrusivi in caso di mancato conferimento di determinate informazioni.

Il Garante ha, in primo luogo, preso atto che in base alla convenzione in fase di applicazione tra l'Agenzia delle entrate e la Rai, quest'ultima può affidare a persone fisiche lo svolgimento di attività di promozione degli abbonamenti radiotelevisivi, anche attraverso contratti di agenzia, designandole come incaricati del relativo trattamento di dati personali.

Sotto il profilo della correttezza del trattamento, il Garante ha prescritto all'Agenzia delle entrate, per ciò che concerne l'attività svolta per suo conto da Rai, l'adozione entro il 30 aprile 2008 di misure che garantiscano che il trattamento dei dati personali, effettuato a cura degli incaricati suddetti, sia conforme ai princìpi del Codice. Ciò, in particolare, deve avvenire evitando induzioni in errore degli interessati, come pure eventuali artifici, anche per quanto concerne le informazioni che gli agenti forniscono ai medesimi interessati circa la propria attività, le proprie qualità e le proprie effettive funzioni di incaricati del trattamento di dati per finalità di promozione degli abbonamenti radiotelevisivi.

L'informativa sul trattamento dei dati personali fornita preventivamente agli interessati deve recare corrette indicazioni circa la reale obbligatorietà o facoltatività del conferimento di dati.

Nelle sollecitazioni rivolte di persona agli interessati, inoltre, deve essere evitata l'indebita prospettazione di controlli intrusivi in caso di mancato conferimento da parte degli stessi di dati di carattere personale.

L'Autorità si è riservata, nell'ambito di un autonomo procedimento, la verifica della corretta predisposizione delle misure di sicurezza relative al trattamento dei dati personali svolto per il recupero dell'evasione del canone radiotelevisivo.

# 14 Sicurezza dei dati e dei sistemi

## 14.1. *Conservazione dei dati di traffico: misure e accorgimenti a garanzia dei cittadini*

Il tema della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati è stato al centro dell'attenzione dell'Autorità anche nel 2007.

Consapevole dei rischi per la libertà e la segretezza delle comunicazioni derivanti da banche dati di enormi dimensioni e in cui confluiscono informazioni particolarmente delicate, il Garante ha adottato quattro *provvedimenti* prescrittivi e di divieto nei riguardi dei principali gestori telefonici (Telecom Italia S.p.A., Vodafone Omnitel N.V., Wind telecomunicazioni S.p.A. e H3G S.p.A.), nonché un *provvedimento* di carattere generale ai sensi dell'art. 132 del Codice. Tali decisioni sono state assunte dopo complessi accertamenti ispettivi volti a verificare il rispetto, da parte dei gestori, delle misure e degli accorgimenti in materia di sicurezza prescritti con i *provvedimenti* del 15 dicembre 2005 [doc. *web* n. 1203890] e del 20 settembre 2006 [doc. *web* n. 1341009] nell'esecuzione di intercettazioni telefoniche e telematiche disposte dall'autorità giudiziaria (*cfr.* *Relazione* 2005, *par.* 15.7 e *Relazione* 2006, *par.* 1.1.1). Limitatamente a Telecom Italia S.p.A., la verifica da parte del Garante ha riguardato anche l'adempimento delle prescrizioni fornite con il *provvedimento* del 1 giugno 2006 ([doc. *web* n. 1296533], *v.* *Relazione* 2006, *p.* 3 *ss.*), finalizzato all'adozione di specifiche misure per rendere trasparente e controllato l'accesso ai *database* contenenti i tabulati di traffico (*cfr.* anche il *Provv.* 7 dicembre 2006 [doc. *web* n. 137104], che ha differito di 90 giorni i termini di adozione delle misure impartite).

**Provvedimenti adottati nei riguardi dei singoli gestori**

L'attività svolta nei confronti di Telecom Italia S.p.A., Vodafone Omnitel N.V., Wind telecomunicazioni S.p.A. e H3G S.p.A. ha fatto emergere alcuni profili critici sul rispetto della normativa e comportato la denuncia all'autorità giudiziaria di due compagnie per mancata adozione di misure minime di sicurezza.

In particolare, il Garante ha prescritto a Telecom, Vodafone e H3G, la cancellazione delle informazioni riguardanti i siti Internet visitati dai relativi abbonati e ha impartito a Vodafone, H3G e Wind l'adozione di specifiche misure tecniche per la messa in sicurezza dei dati personali conservati a fini di giustizia.

I fornitori di accesso alla rete Internet devono infatti conservare esclusivamente i dati di traffico strumentali alla fornitura e alla fatturazione del servizio di connessione e non quei dati apparentemente "esterni" alla comunicazione (pagine *web* visitate o gli indirizzi Ip di destinazione), che possono peraltro, in diversi casi, coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

Più precisamente, nei riguardi di Telecom, il Garante ha imposto anche la cancellazione di dati che talvolta comprendevano persino le interrogazioni ai motori di ricerca effettuate dagli utenti. Alla società è stato inoltre vietato l'uso di sistemi informatici (*proxy server*) non necessari né all'instradamento della comunicazione, né alla fatturazione e che, interponendosi tra l'utente e i siti, consentivano un'ingente raccolta di dati relativi alle connessioni effettuate nel corso della navigazione.

Nei confronti di Vodafone, il Garante ha anche impartito una serie di prescrizioni relative al rispetto delle misure di sicurezza previste dal Codice, all'adozione di

sistemi tecnologici richiesti dal ricordato *provvedimento* del Garante del dicembre 2005, e a ulteriori criticità rilevate nel corso delle ispezioni.

Analogamente nei riguardi di H3G, il Garante ha anche prescritto l'adozione di misure di sicurezza e di ulteriori accorgimenti tecnici in relazione ai profili emersi nel corso degli accertamenti ispettivi.

L'Autorità ha infine prescritto a Wind l'adozione di specifiche cautele relative al rispetto delle misure di sicurezza dettate dal Codice e dal *provvedimento* del 2005, nonché ad ulteriori profili di illiceità del trattamento riscontrati.

**Conservazione dei dati di traffico: misure e accorgimenti a tutela degli interessati**

Prima del recente recepimento in Italia della direttiva 2006/24/Ce in materia di conservazione dei dati di traffico (che prevede un periodo minimo di sei mesi e massimo di due anni), i tempi di conservazione obbligatoria per le finalità di accertamento e repressione dei reati erano di circa 8 anni, per il traffico telefonico, e quasi 4 anni, per quello telematico (*cfr.* d.l. 27 luglio 2005, n. 144, convertito in legge dall'art. 1 della l. 31 luglio 2005, n. 155 e successive modificazioni).

Tale situazione desta preoccupazione in ragione dei pericoli connessi a una così ampia e prolungata conservazione di dati relativi a milioni di persone.

L'intensità dei flussi di comunicazione comporta la formazione di innumerevoli informazioni con una *"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore"* (*cfr.*, fra l'altro, *Corte cost.* 11 marzo 1993, n. 81 e 14 novembre 2006, n. 372) e che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali, e istituzionali.

Eventuali abusi (quali quelli emersi di recente, allorché sono stati constatati gravi e diffusi fenomeni di utilizzo illecito di dati), possono comportare serie ripercussioni sulla riservatezza degli individui o violare segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità di assicurare che la conservazione di tali dati da parte dei fornitori, necessaria per prestare un servizio ovvero imposta dalla legge, avvenga nel rispetto dei diritti e delle libertà delle persone.

Per tali ragioni, con il *provvedimento* di carattere generale del 17 gennaio 2008 [doc. *web* n. 1482111], l'Autorità ha prescritto ai fornitori di servizi di comunicazione elettronica l'adozione, entro il 31 ottobre 2008, di dettagliate misure organizzative e di sicurezza, volte a garantire un elevato livello di protezione dei dati di traffico telefonico e telematico conservati sia per finalità di giustizia, sia per le altre finalità ammesse dalla normativa (art. 123 del Codice).

Tale *provvedimento*, adottato all'esito dei complessi accertamenti ispettivi di cui sopra si è accennato, ha tenuto conto anche delle osservazioni e dei commenti pervenuti a seguito di una consultazione pubblica indetta dall'Autorità su un documento preliminare nel quale era stato delineato un primo quadro regolamentare della materia.

Come è noto, per i fornitori di servizi di comunicazione elettronica è previsto l'obbligo di conservare i dati relativi al traffico per finalità di accertamento e repressione di reati nel rispetto di specifiche misure ed accorgimenti a garanzia dell'interessato (*cfr.* artt. 17 e 132 del Codice), la cui individuazione è stata demandata dal legislatore al Garante (art. 132, comma 5 del Codice).

Il *provvedimento* del 17 gennaio 2008 chiarisce l'ambito di applicazione dell'obbligo di conservazione.

Sul piano soggettivo, per *"fornitore"* sul quale incombe l'obbligo deve intendersi chi mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione; per *"servizi di comunicazione elettronica"* devono intendersi quelli consistenti, esclusivamente o prevalentemente, *"nella trasmissione di segnali su reti di comunicazioni elettroniche"*. Sono pertanto esclusi da tale obbligo i

gestori di esercizi pubblici e *Internet café*, i gestori di siti Internet che diffondono contenuti sulla rete (*"content provider"*), i gestori dei motori di ricerca, le aziende o le amministrazioni pubbliche che mettono a disposizione del personale reti telefoniche e informatiche (*ad es.*, centralini aziendali) o che si avvalgono di *server* resi disponibili da altri soggetti.

Quanto all'ambito oggettivo, l'obbligo riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, nonché i dati inerenti al traffico telematico, esclusi comunque i contenuti delle comunicazioni. In particolare, sono oggetto di conservazione i soli dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione. Il *provvedimento* richiama pertanto i fornitori a conservare, per esclusive finalità di giustizia, i dati di traffico che risultino nella loro disponibilità in quanto derivanti da attività tecniche strumentali alla resa dei servizi offerti dai medesimi, nonché alla loro fatturazione. Il Garante rinvia poi all'art. 5 della direttiva 2006/24/Ce che contiene un'elencazione delle informazioni da conservare e individua diverse categorie di dati di traffico, a seconda si tratti di traffico telefonico (chiamate telefoniche, servizi supplementari, messaggeria e servizi multimediali) o telematico (accesso alla rete Internet, posta elettronica, *fax* nonché messaggi *Sms* e *Mms* via Internet; telefonia via Internet).

L'Autorità ricorda che i dati conservati per gli scopi di cui all'art. 132 del Codice possono essere utilizzati solo per accertamento e repressione di reati. Pertanto, ad esempio, i fornitori non possono corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile; è tenuto a rispettare questo vincolo di finalità anche l'interessato, che può esercitare i diritti di cui all'art. 7 del Codice solo in riferimento a finalità penali.

Il Garante precisa poi di aver individuato gli accorgimenti ritenuti idonei per la conservazione tenuto conto in particolare dell'esigenza normativa volta a prevedere specifiche misure rapportate alla quantità e qualità dei dati da proteggere; dell'opportunità di individuare misure protettive che siano verificabili anche in sede ispettiva; dei costi derivanti dall'adozione delle misure e degli accorgimenti prescritti, anche in ragione della variegata capacità tecnica ed economica dei soggetti interessati; del contesto europeo di riferimento, specie alla luce dei pareri resi dal Gruppo art. 29 che riunisce i Garanti europei; dello stato di evoluzione tecnologica.

Le cautele prescritte dall'Autorità lasciano ai fornitori la facoltà di scegliere l'architettura informatica più idonea per la conservazione obbligatoria dei dati di traffico e per le ordinarie elaborazioni aziendali. I dati di traffico conservati per un periodo non superiore a sei mesi dalla loro generazione possono essere trattati con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti (fatturazione, commercializzazione, *ecc.*), oppure duplicati per effettuare un trattamento dedicato esclusivamente al perseguimento delle finalità di giustizia. In quest'ultimo caso, le misure e gli accorgimenti prescritti per i dati conservati per esclusive finalità di giustizia si applicano sin dall'inizio del trattamento.

In questo quadro, il trattamento dei dati di traffico telefonico e telematico deve essere consentito solo a specifici incaricati, previo utilizzo di sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione. Per i dati conservati per esclusive finalità di giustizia (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), una di tali tecnologie deve essere, poi, basata su caratteristiche biometriche dell'incaricato. Tali cautele trovano applicazione anche per gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possono esserne esonerati solo in circostanze eccezionali (*ad es.*, guasti, aggior-

namento, *ecc.*). In tali casi, tuttavia, deve essere tenuta preventivamente traccia in un apposito "registro degli accessi" dell'evento, nonché delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici.

Salvo quanto sarà aventualmente previsto a sèguito del recepimento della direttiva i profili di autorizzazione devono differenziare le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati, distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice), dagli incaricati abilitati anche al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice). Ciò, ha chiarito il Garante, non determina la moltiplicazione degli addetti ai servizi per scopi di giustizia, potendo lo stesso incaricato ricevere entrambi i profili di autorizzazione.

Con riferimento alle modalità di conservazione, il Garante ha precisato che i dati di traffico trattati per esclusive finalità di giustizia vanno conservati in sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità. Le relative attrezzature informatiche devono essere collocate all'interno di aree ad accesso selezionato e munite di dispositivi elettronici di controllo o di procedure di vigilanza. Nel caso di trattamenti relativi a dati di traffico telefonico, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico.

Quanto ai controlli, l'Autorità ha prescritto che ogni operazione compiuta dagli incaricati o dagli amministratori di sistema sia tracciata e registrata in appositi *audit log*. Devono essere, poi, effettuati controlli periodici sulla legittimità degli accessi ai dati da parte degli incaricati, sul rispetto delle norme di legge e delle misure organizzative tecniche e di sicurezza prescritte, nonché sull'effettiva cancellazione dei dati una volta decorsi i termini di conservazione.

Infine, contro rischi di acquisizione indebita, anche fortuita, delle informazioni registrate da parte di incaricati di mansioni tecniche (amministratori di sistema, amministratori di *database*, manutentori *hardware* e *software*), il Garante ha prescritto che i dati di traffico trattati per esclusive finalità di giustizia siano protetti con tecniche crittografiche.

L'Autorità ha da ultimo esteso l'applicazione di alcune misure e accorgimenti anche ai *database* contenenti dati di traffico conservati per finalità diverse e, segnatamente, per scopi di fatturazione, di commercializzazione di servizi, di statistica, *ecc.* (art. 123 del Codice). Ciò, al fine di favorire un quadro più ampio di sicurezza di dati e sistemi (*strong authentication*, separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati; procedure di cancellazione dei dati allo scadere dei termini previsti dalle disposizioni vigenti; controlli sulle attività poste in essere dagli incaricati; documentazione dei sistemi informativi secondo i princìpi dell'ingegneria del *software*).

**Monitoraggio delle reti *peer to peer*: caso Peppermint**

Nel corso del 2007 numerosi utenti italiani che utilizzano sistemi di *file sharing* si sono visti recapitare, dopo che l'autorità giudiziaria aveva imposto ad alcuni gestori telefonici la comunicazione dei loro dati identificativi, note raccomandate da parte della casa discografica Peppermint contenenti richieste di risarcimento del danno per violazione del diritto d'autore.

Al riguardo sono pervenuti all'Autorità numerosi reclami e segnalazioni, relativi ad asserite violazioni della normativa sulla protezione dei dati personali commesse da tre società (Peppermint Jam Records GmbH, casa discografica con sede in

Germania; Techland sp. z. o.o., società che elabora e commercializza giochi elettronici con sede in Polonia; Logistep AG, con sede in Svizzera che ha svolto un'attività di monitoraggio delle reti *peer to peer* tramite un *software* proprietario). Data l'importanza della questione, il Garante ha ravvisato l'esigenza di costituirsi in alcuni giudizi instaurati presso il Tribunale di Roma con i quali le società Peppermint e Techland sp. z. o.o. intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica la comunicazione delle generalità di soggetti ritenuti responsabili di avere scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer*. I ricorsi si basavano sull'attività svolta per conto e su autorizzazione delle predette società da Logistep AG, che aveva individuato numerosi indirizzi Ip i cui titolari erano stati considerati responsabili della predetta condotta.

Dopo alcune iniziali pronunce favorevoli alle società ricorrenti, il Tribunale di Roma, anche a seguito della costituzione in giudizio del Garante, ha respinto i ricorsi (ordinanza 14 luglio 2007, in causa Peppermint e Techland c/ Wind Telecomunicazioni S.p.A.; ordinanza 14 luglio 2007, in causa Peppermint e Techland c/ Telecom Italia S.p.A.; ordinanza 26 ottobre 2007, in causa Peppermint c/ Wind Telecomunicazioni S.p.A.).

Il Tribunale, pronunciandosi in tema di interpretazione e applicazione dell'art. 156-*bis* della legge n. 633/1941 (introdotto dall'art. 3 del d.lg. n. 140/2006), ha statuito, come richiesto dall'Autorità, che i fornitori di servizi di comunicazione elettronica, allo stato della legislazione vigente, non possono comunicare in sede giurisdizionale civile ai soggetti titolari del diritto d'autore i nominativi degli interessati ritenuti responsabili di violazioni del diritto d'autore in rete. Ciò, stante la specifica disciplina della conservazione dei dati di traffico, prevista solo per finalità di accertamento e repressione dei reati dall'art. 132 del Codice (*v.* anche artt. 5 e 15 della direttiva 2002/58/Ce), ritenuto costituzionalmente legittimo nella parte in cui opera il bilanciamento fra il diritto alla riservatezza e le esigenze di tutela di beni della collettività prevalenti minacciati da gravi illeciti penali (*Corte cost.* n. 372/2006).

Il Garante ha quindi avviato una specifica istruttoria per verificare la liceità e la correttezza dei trattamenti di dati personali posti in essere dalle predette società.

All'esito di tale istruttoria, l'Autorità, con *provvedimento* del 28 febbraio 2008 [doc. *web* n. 1495246], richiamando anche la decisione dell'omologa autorità svizzera (*cfr. www.edoeb.admin.ch*), ha ritenuto illecito il monitoraggio sistematico delle reti *peer to peer* (P2p) svolto per individuare gli utenti che si scambiano illegalmente contenuti protetti dal diritto d'autore (nel caso di specie, *file* musicali e giochi).

Il Garante ha ricordato anzitutto che la direttiva europea sulle comunicazioni elettroniche vieta ai privati di effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti.

L'Autorità ha, inoltre, ritenuto violato anche il principio di finalità, essendo le *cd.* "reti P2p" finalizzate allo scambio tra utenti di dati e *file* per scopi personali. L'utilizzo dei dati dell'utente può dunque avvenire soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè, il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno); ha infine ritenuto non rispettati i princìpi di trasparenza e correttezza, perché i dati erano stati raccolti ad insaputa sia degli interessati, sia di abbonati non necessariamente coinvolti nello scambio di *file*.

Il Garante ha pertanto vietato l'ulteriore trattamento dei dati personali relativo a soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer* e ne ha disposto la cancellazione entro il termine del 31 marzo 2008.

Occorre sottolineare su una questione per molti aspetti simile alla vicenda italiana si è pronunciata la Corte di giustizia delle Comunità europee (sentenza 29 gennaio 2008, causa C-275/06 Promusicae c/ Telefónica de España Sau).

In tale sede la Corte ha confermato che il diritto comunitario consente agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale –ad esclusione, quindi, dei processi civili– il dovere di conservare e mettere a disposizione i dati sulle connessioni e il traffico generati dalle comunicazioni. La Corte ha rilevato che anche i dati di traffico conservati per finalità di fatturazione non possono essere utilizzati in *"controversie diverse da quelle insorgenti tra i fornitori e gli utilizzatori, relative ai motivi della memorizzazione dei dati avvenuta per attività previste dalle disposizioni dell' art. 6 della direttiva 2002/58/Ce"* (*cfr.* art. 123 del Codice); ha, pertanto, escluso la possibilità che tali dati potessero essere messi a disposizione per controversie civili relative ai diritti di proprietà intellettuale (*cfr.* punto 48 della sentenza; artt. 15, n. 2, e 18 della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; artt. 8, n. 1 e 2 direttiva 2001/29/Ce sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; art. 8 direttiva 2004/48/Ce sul rispetto dei diritti di proprietà intellettuale; artt. 17, n. 2 e 47 Carta dei diritti fondamentali dell'Unione europea).

**Pubblicazione di dati personali in Internet**

Sul delicato tema della pubblicazione di dati personali in Internet meritano menzione in particolare due decisioni.

La prima (*Nota* 16 maggio 2007) è stata adottata a seguito di un reclamo proposto da un deputato che lamentava la pubblicazione su una pagina *web* del sito Internet *http://italy.indymedia.org* di una lista di parlamentari che sarebbero risultati positivi al *cd. "test drug-wipe"* (effettuato con modalità che questa Autorità ha ritenuto illecita) nella quale appariva anche il suo nome. L'interessato riconduceva la diffusione di questi dati al *test* effettuato da alcuni inviati della trasmissione televisiva "Le Iene" e lamentava la non veridicità dei dati diffusi, sulla base del presupposto che egli non era *"mai stato oggetto delle inchieste e delle interviste effettuate dagli inviati della trasmissione Le Iene"*.

Dagli accertamenti compiuti dall'Ufficio era emerso che tali informazioni risultavano essere state inserite in rete antecedentemente al *provvedimento* inibitorio del Garante adottato nei confronti della società editrice del predetto programma televisivo. Al *provvedimento* di blocco adottato in via d'urgenza dall'Autorità in data 10 ottobre 2006 [doc. *web* n. 1345622] aveva fatto seguito un ulteriore *provvedimento* (adottato il 14 dicembre 2006 [doc. *web* n. 1370781]) che, sulla base di un compiuto esame del merito, aveva accertato la mancanza di liceità e correttezza nel trattamento (*v. Relazione* 2006, *p.* 79 *ss.*). Nella pagina *web* diffusa non risultava inoltre specificato che le informazioni ivi pubblicate erano state acquisite utilizzando i *test* effettuati dagli inviati della trasmissione "Le Iene". Ancora, dalle informazioni disponibili risultava che la pagina *web* era stata inserita in un *forum* di discussione (*cd. "newswire"*, ossia *"uno spazio informativo a pubblicazione aperta"*) presente su un sito Internet (*www.indymedia.org*), già in passato oggetto di un provvedimento da parte dell'autorità giudiziaria, i cui *server* risultavano ubicati negli Stati uniti d'America e il cui nome a dominio risultava registrato da un soggetto residente in Brasile. Infine, il trattamento contestato non risultava riconducibile a persone fisiche individuabili, essendo stati utilizzati alcuni *alias*. Tuttavia, non si poteva escludere che tali persone fossero stabilite sul territorio dello Stato italiano, in ragione di alcuni elementi fra i quali la lingua utilizzata, il fatto che la sezione del *forum* fosse stata dedicata specificamente al pubblico italiano (*Italy Indymedia*) e a questioni attinenti alla vita politica e sociale italiana.

Il Garante ha pertanto rilevato che solo laddove fosse pienamente comprovato questo presupposto, poteva essere configurabile un intervento dell'Autorità nei confronti delle predette persone (*cfr.* art. 5 del Codice); non emergevano, invece, allo stato degli atti, i presupposti giuridici per consentire un intervento diretto nei riguardi del gestore del sito. L'Autorità ha quindi prospettato al reclamante, ferma restando la possibilità di adire anche l'autorità giudiziaria ordinaria per eventuali profili di carattere penale, di rivolgersi direttamente al gestore del sito Internet, richiedendo la rimozione immediata dei contenuti ritenuti illeciti. Ciò, anche in relazione a una prassi nota come *"notice and take down"*, applicata in altri ambiti normativi per proteggere i titolari di diritti d'autore e introdotta negli Stati uniti dal *Digital Millenium Copyright Act* nonché, in ambito comunitario, dalla direttiva 2000/31/Ce (relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, e recepita in Italia con il d.lg. n. 70/2003).

La seconda decisione (*Nota* 16 maggio 2007) è stata, invece, adottata a seguito di una segnalazione che lamentava la diffusione via Internet di notizie considerate inesatte e diffamatorie.

In tale occasione il Garante ha ricordato i contatti avviati con la società Google Inc., con sede negli Stati uniti, per individuare soluzioni volte a garantire i diritti della persona interessata, anche quando il titolare del trattamento effettuato sia stabilito fuori dell'Unione europea e non sia pertanto soggetto all'applicazione del Codice. Il Garante, in particolare, ha ricevuto formali assicurazioni circa la disponibilità della società statunitense a rendere più agevole e tempestiva la cancellazione delle pagine *cache* (copie delle pagine originali) e dei relativi "titoli" e "sommarietti" reperibili con il motore di ricerca, quando, però, le pagine originali non sono più presenti presso i siti *web* "sorgente", ossia i siti dai quali sono estratte le copie *cache* (*cfr. Comunicato stampa* 30 maggio 2006). L'Autorità ha, pertanto, sollecitato il segnalante, relativamente agli articoli pubblicati in Italia, a esercitare i diritti di rettifica di dati erronei o di aggiornamento e integrazione nei riguardi dell'editore titolare del trattamento ai sensi dell'art. 7 del Codice. In particolare, ha suggerito di chiedere (art. 7, comma 1, lett. *c*) del Codice), l'attestazione che le operazioni di cui sopra siano state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi (ossia, nel caso di specie, Google Inc.). A tale riguardo, ha inoltre ricordato che il *webmaster* del sito "sorgente" può anche utilizzare alcuni meccanismi di rimozione di "contenuti obsoleti" messi a sua disposizione da Google.

### 14.2. *Prescrizioni sulla sicurezza dei dati negli uffici giudiziari*

Come riferito nella *Relazione* 2006, il Garante ha preso in esame anche l'applicazione delle misure di sicurezza nei trattamenti dei dati personali cartacei e automatizzati, di tipo amministrativo e per ragioni di giustizia, effettuati presso gli uffici giudiziari, nella convinzione che l'introduzione di livelli elevati di sicurezza in tali trattamenti contribuisce anche al buon funzionamento delle strutture giudiziarie.

In tale ambito, l'Autorità ha deliberato di effettuare una prima serie di accertamenti in relazione ai trattamenti di dati personali svolti, per motivi di giustizia (art. 47, comma 2, del Codice), presso il Tribunale ordinario di Roma, limitatamente, in una prima fase, al settore civile (*Provv.* 1 febbraio 2007, [doc. *web* n. 1385301]). Gli accertamenti, intrapresi nei modi previsti dalla legge, con la presenza di un componente del Garante da questo designato e con l'assistenza di personale specializzato

(art. 160 del Codice), si sono protratti nell'arco del 2007 mediante l'acquisizione di informazioni e documentazione e attraverso numerose verifiche e sopralluoghi svolti, con la piena collaborazione della magistratura e del personale amministrativo, presso tutte le sezioni civili e il settore informatico del Tribunale.

Le risultanze degli accertamenti costituiscono parte integrante della motivazione del *provvedimento* del 15 novembre 2007 con il quale il Garante, ravvisata l'esigenza di rafforzamento del livello di protezione dei dati, ha indicato al Tribunale ordinario di Roma la necessità di apportare alcune modificazioni e integrazioni alle misure di sicurezza concernenti il trattamento dei dati gestiti con strumenti elettronici e contenuti nei fascicoli processuali.

L'Autorità ha disposto di inviare copia del provvedimento al Ministero della giustizia con riferimento alle pertinenti competenze in tema di organizzazione e funzionamento dei servizi relativi alla giustizia, e al Consiglio superiore della magistratura, per ogni opportuna conoscenza in relazione alle relative attribuzioni.

# 15 La videosorveglianza e la biometria

## 15.1. *Videosorveglianza in ambito privato*

**Verifiche preliminari**

Nonostante i ripetuti interventi del Garante, a distanza di circa quattro anni dall'adozione del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482] sono continuate a giungere diverse richieste di verifiche preliminari sull'installazione di impianti di videosorveglianza da parte di soggetti privati.

Al riguardo, in più circostanze è stato ribadito che devono essere sottoposti a esame preventivo dell'Autorità solo i trattamenti connessi ad alcuni sistemi (specificamente individuati al punto 3.2 del menzionato *provvedimento*) quali i sistemi di videosorveglianza *cd.* "dinamico-preventiva", ovvero quelli che prevedono una raccolta delle immagini collegata e/o incrociata e/o con altri particolari dati personali. Pertanto, gli impianti installati in conformità alla disciplina di protezione dei dati personali e alle prescrizioni contenute nel citato *provvedimento* non devono essere oggetto di alcuna verifica preliminare da parte dell'Autorità.

Tale profilo è stato oggetto di approfondimento anche in occasione di un incontro presso la sede dell'Autorità tenutosi con la Federazione nazionale imprese elettrotecniche ed elettroniche (Anie), in rappresentanza dei principali produttori ed installatori di sistemi di videosorveglianza. Le questioni ivi sollevate, allo stato oggetto di analisi e studio da parte dell'Autorità, concernono principalmente i casi in cui risulta necessario procedere a una richiesta di verifica preliminare *ex* art. 17 del Codice in ragione di alcune specifiche caratteristiche tecniche degli impianti di videosorveglianza attualmente in commercio (quali la digitalizzazione/indicizzazione delle immagini), nonché dei profili connessi alle misure di sicurezza e all'attestazione di conformità dei sistemi (regola 19 Allegato B del Codice). A quest'ultimo proposito l'Associazione ha rappresentato l'opportunità di predisporre, anche a seguito di un'attività collaborativa con l'Autorità, una modellistica utilizzabile dalla pluralità di soggetti che possono intervenire nelle fasi di produzione, progettazione, e installazione del sistema di videosorveglianza.

Ulteriore aspetto oggetto di riflessione da parte dell'Autorità, anche alla luce di talune segnalazioni pervenute, è poi quello legato all'identificazione di tempi congrui di conservazione dei dati registrati, al di là dei limiti temporali indicati, in assenza di una disciplina di settore che regoli il delicatissimo settore della videosorveglianza negli spazi pubblici, nel già citato *provvedimento* generale del 2004.

**Vigilanza negli spogliatoi**

A seguito della denuncia di un furto avvenuto all'interno degli spogliatoi di una piscina, i Carabinieri hanno acquisito la videocassetta delle riprese effettuate da un sistema di videosorveglianza che si avvaleva di due coppie di telecamere, entrambe visibili, e ne hanno dato notizia al Garante. È emerso in particolare che le telecamere, oltre a controllare la zona adibita a guardaroba, riprendevano direttamente le persone anche mentre si cambiavano gli indumenti.

Nonostante la presenza delle telecamere fosse segnalata, l'Autorità ha ravvisato la violazione della riservatezza e della dignità delle persone (art. 2 del Codice) in quanto, pur essendo lecito l'utilizzo di sistemi di videosorveglianza per tutelarsi da eventuali danni o furti, non erano stati adottati accorgimenti volti a evitare riprese indebite di persone negli spogliatoi.

Il Garante ha quindi disposto il divieto di installare telecamere con le modalità indicate e ha bloccato il trattamento dei dati già raccolti, nelle more di eventuali altre attività di accertamento da parte delle competenti autorità; ha poi prescritto al titolare del trattamento il rispetto dei princìpi generali in materia di sistemi di videosorveglianza e protezione dei dati stabiliti nel *provvedimento* del 29 aprile 2004 [doc. *web* n. 1003482], sottolineando in particolare l'obbligo di adottare tutte le misure necessarie per evitare la ripresa delle persone negli spogliatoi e per assicurare un'adeguata informativa ai clienti sulla presenza di telecamere (*Provv.* 8 marzo 2007 [doc. *web* n. 1391803]).

**Videosorveglianza sui luoghi di lavoro**

In relazione ad alcune generiche segnalazioni sull'installazione di impianti di videosorveglianza in violazione dello Statuto dei lavoratori (art. 4 l. n. 300/1970), il Garante ha ricordato, in base alla specifica normativa di settore (fatta peraltro salva dall' art. 114 del Codice), la competenza delle direzioni provinciali del lavoro.

Sotto altro profilo, non sono stati ravvisati elementi per un intervento da parte dell'Autorità in ordine ad un impianto di videosorveglianza installato presso alcune zone di transito e d'ingresso agli uffici di una società di trasporto pubblico locale. All'esito dei preliminari accertamenti effettuati dal Garante, infatti, la società ha dichiarato, ai sensi e per gli effetti di cui all' art. 168 del Codice, che il sistema informativo e il relativo programma informatico erano stati conformati in modo tale da non utilizzare dati relativi a persone identificate o identificabili (con esclusione, pertanto, della possibilità di ingrandire le immagini) (*Nota* 23 gennaio 2008).

**La videosorveglianza nei condomìni**

Il trattamento connesso all'installazione di sistemi di ripresa nelle aree comuni di edifici condominiali e loro pertinenze è oggetto di ulteriori approfondimenti da parte del Garante, in considerazione delle ampie fasce di popolazione coinvolta e della necessità di tutelare il diritto alla riservatezza e le libertà personali in prossimità dei luoghi adibiti a privata dimora.

In particolare, le questioni sollevate, solo in parte oggetto di intervento da parte del Garante con il *provvedimento* del 29 aprile 2004 [doc. *web* n. 1003482] e non chiaramente risolte dal codice civile, riguardano soprattutto le operazioni di trattamento conseguenti all'installazione di sistemi di videosorveglianza da parte dell'intera compagine condominiale all'interno di aree comuni quali, portoni d'ingresso, androni, cortili, scale, aree comuni di accesso ai parcheggi, al fine di preservare la sicurezza di persone e la tutela di beni comuni (*ad es.*, contro aggressioni o danneggiamenti e furti).

**Finalità esclusivamente personali**

È stato inoltre chiarito che la disciplina di protezione dei dati non trova applicazione in caso di trattamenti effettuati per fini esclusivamente personali, purché le immagini registrate non siano oggetto di successiva comunicazione sistematica o diffusione (*cfr.* art. 5, comma 3 del Codice). Peraltro, considerato che numerose segnalazioni avevano ad oggetto l'installazione di impianti di videosorveglianza in ambito condominiale, questa Autorità ha provveduto a puntualizzare che, onde evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.), l'angolo visuale delle riprese deve essere limitato ai soli spazi di esclusiva pertinenza del singolo condomino (*ad es.* antistanti l'accesso alla propria abitazione), escludendo ogni forma di ripresa, anche senza registrazione, di immagini relative ad aree comuni (cortili, pianerottoli, scale, garage comuni) o riferite ad aree antistanti l'abitazione di altri condomini. Una specifica segnalazione è stata da ultimo inoltrata al Parlamento e al Governo.

### 15.2. *Biometria in ambito pubblico*

Nel 2007 è stata completata l'ampia istruttoria sull'utilizzo, da parte di soggetti pubblici, di sistemi di riconoscimento delle impronte digitali dei dipendenti per il controllo degli accessi sui luoghi di lavoro.

Le conclusioni di tale attività sono confluite nel *provvedimento* generale sul trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In particolare, il citato *provvedimento* evidenzia che l'utilizzo generalizzato di sistemi di rilevazione automatica delle presenze dei dipendenti mediante la raccolta di dati biometrici ricavati dalle impronte digitali non è consentito ove siano attivabili misure "convenzionali" non lesive dei diritti della persona. Inoltre non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di note relative a progetti di installazione di impianti di rilevazione di impronte digitali, cui eventualmente non segua un esplicito riscontro dell'Autorità.

Tali chiarimenti sono stati forniti ai diversi segnalanti che si erano rivolti all'Autorità e alle numerose amministrazioni pubbliche che avevano inoltrato specifiche richieste di parere al riguardo (*Note* 11 luglio 2007, 18 luglio 2007, 20 luglio 2007, 26 luglio 2007, 30 luglio 2007, 1 agosto 2007, 9 ottobre 2007, 7 dicembre 2007, 10 dicembre 2007 e 18 dicembre 2007).

Un ente locale ha posto un quesito su un sistema di riconoscimento biometrico dell'impronta digitale per l'utilizzo di *personal computer* dei dipendenti abilitati ad accedere ai dati sensibili presenti nelle banche dati. L'impronta sarebbe stata memorizzata e verificata non come immagine dattiloscopica, ma in forma sintetizzata e complessa (*template*), e poi registrata in una *smart card* nell'esclusiva disponibilità del dipendente. Attraverso tale progetto si sarebbe inteso attivare una credenziale di autenticazione in conformità alla regola n. 2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Codice).

Come in analoghe circostanze, nel caso di specie, non è risultato necessario prescrivere misure o accorgimenti, tenuto conto della sola finalità perseguita di autenticazione informatica. L'adozione di un sistema di autenticazione informatica, mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali, se conforme ai requisiti tecnici indicati dal Codice (*cfr.* regole da 1 a 11 dell'Allegato B al Codice), costituisce infatti una misura minima di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti a utilizzare. Tali credenziali di autenticazione possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave (*cfr. Relazione* 2005, *p.* 113; *Relazione* 2006, *p.* 121; *Nota* 1 giugno 2007).

Una soprintendenza archeologica aveva chiesto che fosse oggetto di verifica preliminare ai sensi dell'art. 17 del Codice un sistema di riconoscimento biometrico basato sul rilevamento delle caratteristiche geometriche della mano per consentire a un numero limitato di dipendenti l'accesso a un'area riservata particolarmente sensibile, al fine di identificarli in modo certo e garantire così *standard* di sicurezza specifici ed elevati, richiesti dalla natura delle attività svolte nell'area riservata.

Il sistema prevedeva l'associazione alle caratteristiche geometriche della mano di un algoritmo crittografico poi archiviato nella memoria interna del dispositivo biometrico. Tale dispositivo non era collegato in rete e poteva essere attivato per effettuare l'accesso solo attraverso una parola chiave numerica scelta dal dipendente.

Il trattamento dei dati in questione è stato ritenuto dall'Autorità lecito e proporzionato allo scopo. Da una parte, l'attività di identificazione rientrava nelle finalità istituzionali della soprintendenza, la quale, dovendo garantire nel caso di specie ele-

vati *standard* di sicurezza, aveva necessità di un rigoroso accertamento dell'identità dei dipendenti. Dall'altra, è stato rilevato che le caratteristiche geometriche della mano di un individuo, a differenza delle impronte digitali utilizzabili anche in altri contesti con effetti sugli interessati, non sono descrittive al punto tale da risultare uniche; possono eventualmente non garantire l'identificazione univoca e certa di una persona, ma sono sufficientemente dettagliate per essere impiegate in circoscritti ambiti ai fini della verifica di identità. La geometria della mano appartiene a quella categoria di dati biometrici che non lasciano tracce suscettibili di essere utilizzate per scopi diversi da quelli perseguiti da chi le raccoglie ed usa.

Nell'autorizzare l'uso del sistema, il Garante ha comunque prescritto di integrare l'informativa ai dipendenti, specificando le modalità alternative di accesso per coloro che non avessero voluto o potuto avvalersi del sistema di rilevazione delle caratteristiche della mano (*Provv.* 8 novembre 2007 [doc. *web* n. 1461908]).

Da ultimo, l'Ufficio (*Nota* 11 marzo 2008) ha fornito alcune indicazioni preliminari su un sistema di distribuzione automatica di tabacchi basato sul riconoscimento dell'impronta digitale.

In un quesito, l'Amministrazione autonoma dei monopoli dello Stato, per evitare l'acquisto di tabacchi lavorati nei distributori automatici da parte di minori infrasedicenni, in specifiche fasce orarie notturne aveva ipotizzato un sistema basato su *smart card* non nominative che memorizzerebbero in forma cifrata l'impronta digitale delle persone che la richiedano, senza identificarle direttamente.

Il quesito non chiariva tutti i dettagli necessari, e perciò nella risposta sono state considerate diverse ipotesi.

Qualora il rivenditore si limitasse a verificare genericamente l'età della persona che richiede la *smart card* (essendo evidente che non si tratti di minore, sulla base di conoscenza personale o della mera esibizione di un documento di identità), il dato relativo all'impronta memorizzata sulla *smart card* avrebbe pur sempre carattere personale, ma non sarebbe necessario sottoporre formalmente il sistema al vaglio preliminare del Garante ai sensi dell' art. 17 del Codice ai fini della prescrizione di particolari misure e accorgimenti a garanzia degli interessati.

In tal caso, quindi, il rivenditore non tratterrebbe alcun dato personale identificativo dei richiedenti (generalità, copie di documenti di identità), apparendo sufficiente che la *smart card* sia in concreto utilizzabile solo dalla persona legittimata (non identificata) che l'ha richiesta. Si dovrebbe allora prevedere (a parte una sintetica informativa agli interessati) che nella *smart card* sia registrato in forma cifrata il solo *template* (forma sintetizzata e complessa) dell'impronta, anziché l'immagine fotografica cifrata dell'impronta stessa, e che si chiariscano i profili relativi all'eventuale tracciamento delle operazioni svolte dalle singole *smart card* e all'eventuale conservazione temporanea dei dati corrispondenti.

Invece, nel caso in cui presso il rivenditore o altrove restasse traccia nominativa dei richiedenti, sarebbe necessario avviare un formale procedimento di verifica preliminare ai sensi del predetto art. 17.

### 15.3. *Videosorveglianza in ambito pubblico*

Anche nel 2007 numerose segnalazioni pervenute al Garante hanno confermato l'attualità delle problematiche relative all'impiego dei sistemi di videosorveglianza da parte dei soggetti pubblici.

Si è reso pertanto necessario fornire talune precisazioni in relazione alle indicazioni contenute nel *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482].

In particolare, in ambito sanitario, a seguito della richiesta di un sindacato, il Garante ha sottolineato che nell'uso di videocamere all'interno di un'azienda sanitaria per finalità di sicurezza si deve evitare accuratamente il rischio di diffondere immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico. L'eventuale controllo di ambienti sanitari deve essere limitato ai casi di stretta indispensabilità, circoscrivendo le riprese solo a determinati locali e a precise fasce orarie e l'accesso alle immagini ai soggetti specificamente autorizzati (*ad es.*, personale medico ed infermieristico) (*Nota* 16 aprile 2007).

In relazione a un quesito di un'azienda sanitaria circa la possibilità di installare un dispositivo di videosorveglianza a circuito chiuso nei servizi igienici del laboratorio di patologia clinica e tossicologica dell'azienda medesima, al fine di evitare che il campione urinario da prelevare potesse essere oggetto di falsificazione da parte del soggetto sottoposto al controllo tossicologico, è stata richiamata l'esigenza di rispettare il principio generale di proporzionalità tra i mezzi impiegati e le finalità perseguite.

Più in particolare, l'Ufficio, nel ricordare che il trattamento di dati personali non deve comportare un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali dei soggetti ripresi, ha evidenziato che l'installazione di una telecamera nei servizi igienici può configurarsi come lesiva della dignità degli individui sottoposti ai controlli e ha richiamato le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (*toilette*, stanze d'albergo, cabine, spogliatoi, *ecc.*) (*Nota* 17 gennaio 2008).

Analoga questione ha riguardato un'altra azienda sanitaria che ha formulato un quesito relativo all'istallazione di sistemi di videosorveglianza con registrazione presso il locale di distribuzione del metadone, al fine di monitorare l'effettiva assunzione del farmaco da parte dell'assistito (*Nota* 26 luglio 2007).

Nel diverso ambito degli istituti scolastici, l'Ufficio ha ribadito la necessità di garantire il rispetto del diritto alla riservatezza dello studente, e ha evidenziato che l'installazione di sistemi di videosorveglianza in ambienti scolastici, potendo comportare la raccolta di dati riguardanti anche minori, deve essere limitata ai casi di stretta indispensabilità. In caso di reale necessità, tali sistemi, in conformità al principio di proporzionalità, devono essere comunque circoscritti alle sole aree interessate ed attivati nell'orario di chiusura dell'istituto (*Nota* 5 luglio 2007).

A un ente locale che intendeva utilizzare *webcam* per finalità turistiche, è stato precisato che, in linea generale, non viola le disposizioni in materia di protezione dei dati personali l'impiego per fini promozionali, turistici o pubblicitari, di *webcam* o *camera on-line* che non consentano di individuare i tratti somatici delle persone riprese (*cfr. Provv.* 29 aprile 2004, già cit. e *Provv.* 14 giugno 2001 [doc. *web* n. 41782]).

In tale occasione il Garante ha avuto anche modo di ricordare che l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo dell'Autorità; non può, pertanto, desumersi alcuna approvazione implicita dalla semplice trasmissione al Garante di comunicazioni o di progetti relativi all'installazione di sistemi di videosorveglianza. Non è infatti stabilito alcun termine decorso il quale i progetti sottoposti alla verifica dell'Autorità possano ritenersi autorizzati, non applicandosi al riguardo il principio del silenzio-assenso (*Nota* 1 agosto 2007).

L'Autorità, nuovamente interpellata da alcune amministrazioni in ordine alla necessità di sottoporre taluni trattamenti di dati personali alla verifica preliminare, ha ricordato che il *provvedimento* del 29 aprile 2004 individua espressamente le ipotesi in cui i sistemi di videosorveglianza da attivare devono essere sottoposti alla verifica preliminare del Garante. Spetta, quindi, all'amministrazione richiedente valu-

tare se, nell'ambito di una attività di videosorveglianza, vi siano trattamenti rientranti in quelle ipotesi, da sottoporre all'esame preventivo dell'Autorità.

Ad esempio, il normale esercizio di un impianto di videosorveglianza digitale, in cui le immagini vengono riprese da telecamere digitali dotate delle ordinarie funzioni di ricerca, non comporta rischi specifici per gli interessati, essendo funzionalmente analogo alla videosorveglianza tradizionale con registrazione analogica delle immagini su supporti magnetici. Pertanto, l'adozione di sistemi digitali di questo tipo non implica la richiesta di verifica di cui all' *art.* 17 del Codice, necessaria, invece, in caso di utilizzo di tecniche avanzate di indicizzazione e ricerca, miranti al riconoscimento o alla classificazione sulla base di caratteristiche morfologiche e comportamentali degli interessati (*Nota* 2 gennaio 2008).

Da ultimo si menziona la segnalazione di un cittadino che lamentava la presenza di telecamere installate dal comune in grado di effettuare riprese ravvicinate all'interno del suo appartamento.

Le telecamere, come dichiarato dallo stesso comune, erano state posizionate, oltre che per monitorare il traffico, anche per esigenze di maggiore sicurezza dei cittadini, tutela del patrimonio e controllo di determinate aree.

Dagli accertamenti disposti dal Garante è emerso tuttavia che il tipo di telecamera installata permetteva *zoom*, brandeggio e identificazione dei tratti somatici delle persone riprese e che il sistema consentiva a qualsiasi operatore che avesse accesso diretto al *server* di spostare le telecamere nelle diverse direzioni operando così un'ingiustificata intromissione nella vita privata degli interessati.

Valutati questi elementi il Garante ha stabilito che, per utilizzare lecitamente il sistema di videosorveglianza, il comune avrebbe dovuto adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private, delimitando la dislocazione, l'uso dello *zoom* e l'angolo visuale delle telecamere in modo da escludere ogni forma di ripresa, anche in assenza di registrazione, di spazi interni, attraverso eventuali sistemi di "settaggio" e oscuramento automatico, non modificabili dall'operatore. È stato inoltre prescritto di integrare il modello di informativa fornita dal comune indicando, oltre al monitoraggio del traffico, le finalità di sicurezza e di controllo di competenza (*Provv.* 4 ottobre 2007 [doc. *web* n. 1457505]).