17 La videosorveglianza e la biometria

17.1. *L'utilizzo di credenziali biometriche nelle aziende e nei luoghi di lavoro*

In linea con la tendenza delineatasi nel corso dell'anno precedente, nel 2006 sono pervenute ulteriori richieste di verifica preliminare ai sensi dell'art. 17 del Codice riguardanti l'attivazione di credenziali di autenticazione biometrica per l'accesso a sistemi informativi aziendali.

In tale ambito occorre segnalare l'istanza presentata da una multinazionale operante nel settore farmaceutico, interessata ad introdurre un sistema di credenziali di autenticazione dei propri dipendenti basato sull'impiego delle impronte digitali. In base alla sommaria descrizione del progetto fornita dalla società non è risultata necessaria la valutazione preliminare dell'Autorità, tenuto conto della finalità di autenticazione informatica perseguita e della caratteristica biometrica utilizzata nel caso di specie, che non rendeva necessaria la creazione di archivi centralizzati. Come già affermato dal Garante in precedenti circostanze, infatti, ove l'adozione di un sistema di autenticazione informatica (mediante il quale gli incaricati dotati di apposite credenziali, anche biometriche, possono effettuare specifici trattamenti di dati personali) sia conforme ai requisiti tecnici indicati dalle regole 1-11 dell'Allegato B. al Codice, il sistema medesimo costituisce una misura minima di sicurezza che il titolare, il responsabile (se designato) e gli incaricati sono tenuti a predisporre e applicare (art. 34, comma 1, lett. *a*), del Codice).

Nella seconda metà del 2006 è stato sottoposto al vaglio del Garante un progetto basato sull'installazione di un impianto di rilevazione di impronte vocali di lavoratori, per finalità di autenticazione informatica, presso la filiale italiana di una multinazionale operante nel settore della produzione di pneumatici. L'Autorità ha avviato un esame preliminare delle caratteristiche del trattamento di dati personali biometrici al fine di valutare se, nel caso di specie, fosse effettivamente necessario attivare il procedimento di verifica previsto dall'art. 17 del Codice. A questo scopo sono stati richiesti alla società i dettagli del progetto e del connesso trattamento dei dati dei lavoratori, con particolare riguardo al luogo in cui erano ubicati il *server* utilizzato e il *data-base* eventualmente associato (per stabilire se il trattamento fosse effettuato nel territorio nazionale, ovvero in altro Stato dell'Unione europea dove la multinazionale ha la sua sede principale) e al sistema di archiviazione delle impronte vocali utilizzato (per comprendere se il sistema richiedesse la creazione di un archivio centralizzato di tali dati e, in caso affermativo, quali fossero le misure di sicurezza ipotizzate a protezione dei dati biometrici).

In generale, l'attività di valutazione della legittimità dell'impiego dei sistemi di rilevazione biometrica in ambito lavorativo si è intensificata rispetto al 2005. Il Garante ha adottato nuove decisioni a seguito dell'interpello di alcuni titolari del trattamento ai sensi dell'art. 17 del Codice (*cfr.* anche l'art. 20 della direttiva n. 95/46/Ce).

Utilizzo di dati tratti da impronte digitali per controllo accessi ad aree dove si svolgono lavorazioni pericolose

Completata l'istruttoria sugli interpelli presentati da alcune società che svolgono attività industriale di carattere molitorio, interessate a ricorrere all'impiego delle impronte digitali dei propri dipendenti per rilevarne le presenze e controllarne gli accessi a particolari aree produttive, l'Autorità ne ha accolto parzialmente le istanze, prescrivendo specifici accorgimenti da adottare nel trattamento dei dati biometrici dei lavoratori (*Provv.* 15 giugno 2006 [docc. *web* n. 1306523, n. 1306530 e n. 1306551]).

In particolare, riguardo al trattamento di impronte digitali per l'accesso a circoscritte aree produttive contraddistinte dalla pericolosità delle lavorazioni espletate (nella specie, ambienti di lavoro con presenza di atmosfera esplosiva, inclusi nell'elenco delle attività soggette a visite e controlli periodici dei vigili del fuoco al fine del rilascio del certificato di prevenzione incendi di cui al punto 35 del decreto del Ministero dell'interno 16 febbraio 1982 e rientranti, altresì, nell'ambito applicativo di specifiche direttive comunitarie in materia), muovendo dal presupposto che il datore di lavoro è tenuto ad adottare le misure necessarie a tutelare l'integrità fisica dei lavoratori (art. 2087 c.c.; *v.* anche d.lg. n. 626/1994 e successive modifiche ed integrazioni), il Garante ha ritenuto ammissibile limitare l'accesso agli impianti ai soli dipendenti specializzati e addetti alle lavorazioni effettuate in tali aree, anche attraverso la verifica delle loro identità mediante l'impiego di sistemi biometrici.

Nel caso di specie, non è risultato sproporzionato l'uso di dati biometrici tratti dalle impronte digitali, poiché il trattamento veniva effettuato mediante un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il modello (*cd. "template"*), cifrato e memorizzato su un supporto privo di indicazioni nominative riferibili all'interessato e destinato a rimanere nell'esclusiva disponibilità di quest'ultimo.

Il trattamento di dati biometrici è stato invece vietato in relazione al perseguimento della diversa finalità di rilevazione della presenza dei dipendenti, in quanto le società non avevano addotto ragioni specifiche volte a chiarire la necessità dell'utilizzo di tali modalità di trattamento per verificare il puntuale adempimento della prestazione lavorativa. Inoltre, i dispositivi in questione sarebbero stati introdotti solo nei confronti di un gruppo di dipendenti, mentre per i restanti lavoratori le società avrebbero continuato ad avvalersi del sistema già in uso.

L'Autorità ha poi prescritto ai titolari del trattamento di riformulare l'informativa resa ai lavoratori interessati dal trattamento dei dati biometrici, indicandovi con chiarezza le finalità perseguite e gli ulteriori elementi indicati all'art. 13 del Codice. I dati relativi agli orari di accesso agli impianti molitori possono essere ora conservati per il tempo massimo di quarantotto ore.

Impiego di dati biometrici in ambito aeroportuale

Un altro caso sottoposto all'esame del Garante ha riguardato una società che, in possesso della qualifica di "agente di *handling* autorizzato" riconosciuta dall'Ente nazionale per l'aviazione civile-Enac, svolge attività di movimentazione a terra delle merci in ambito aeroportuale.

La società ha presentato una richiesta di verifica preliminare relativa al trattamento di dati biometrici (ricavati dalla lettura delle impronte digitali) del personale che ha accesso ad alcuni locali della propria sede operativa aeroportuale di Milano-Malpensa –un magazzino di stoccaggio delle merci ed un *caveau* nel quale sono depositati beni di particolare valore– ubicati in *cd.* "aree sterili" soggette a controlli e procedure inerenti la tutela della sicurezza e dell'ordine pubblico previsti dal "Programma nazionale di sicurezza" di cui al d.P.R. 4 luglio 1985, n. 461 per esigenze di tutela di persone e cose e di prevenzione del rischio di atti terroristici, nonché da ulteriori prescrizioni di sicurezza impartite dalla direzione di aeroporto. Tali prescrizioni prevedono la possibilità di ingressi per soggetti autorizzati attraverso

varchi configurati in modo da consentire l'accesso ad una persona per volta tramite inserimento del proprio *badge*, associato ad un *pin*, nell'apposito lettore, ovvero previa approvazione dell'Enac, mediante l'utilizzo di sistemi biometrici.

Il sistema di verifica biometrica sottoposto al vaglio del Garante era costituito da dispositivi di lettura di impronte digitali "non centralizzati" e integralmente autonomi nello svolgimento della procedura di identificazione biometrica, nonché da un *software* per la trasformazione in un codice numerico dell'impronta rilevata in occasione di ogni ingresso all'area riservata, codice da confrontare poi con il *template* ricavato dalla lettura dell'impronta dell'interessato e cifrato solo su una *smart card* posta nell'esclusiva disponibilità del lavoratore. L'associazione tra i due codici, preceduta dalla lettura della tessera, avrebbe consentito l'accesso all'area riservata. La società intendeva poi trattare, oltre ai dati biometrici estratti dall'analisi delle impronte digitali, anche il nome e cognome, il numero di matricola, il codice assegnato al *badge* utilizzato quale supporto del *template* e il profilo di autorizzazione individuale.

Nelle intenzioni della società, il sistema biometrico (da installare a presidio di cinque accessi ai locali sopra menzionati, e in grado di garantire un accertamento più rigoroso dell'identità del personale autorizzato ad accedere ai locali sopra menzionati) sarebbe stato utilizzato anche per controllare l'accesso agli uffici della società presenti nell'area aeroportuale e preordinato, altresì, alla rilevazione della presenza dei dipendenti della società medesima.

Gli elementi acquisiti hanno consentito al Garante (*Provv.* 26 luglio 2006 [doc. *web* n. 1318582]) di ritenere lecito e proporzionato il trattamento di dati biometrici per presidiare gli accessi ad "aree sensibili" (magazzino e *caveau*) al fine di assicurare la sicurezza di terzi, non solo in considerazione della peculiarità di tali locali, ma anche in vista delle caratteristiche tecniche del sistema, risultate conformi alle indicazioni fornite in fattispecie di analoga delicatezza (si prevedeva infatti la memorizzazione del *template*, opportunamente crittografato, esclusivamente su una *smart card*).

Di contro, l'Autorità non ha ritenuto conforme ai principi di necessità e proporzionalità (artt. 3 e 11 del Codice) l'utilizzo del medesimo sistema per il controllo dell'accesso ad uffici della società, finalità rispetto alle quali non è stata fornita idonea prova della sussistenza di analoghe stringenti esigenze di sicurezza in grado di giustificare l'utilizzo di dati biometrici in luogo di metodi meno invasivi.

Il trattamento di dati biometrici non è stato ritenuto lecito neppure per il perseguimento della finalità di rilevazione della presenza dei dipendenti, in quanto la società non ha addotto ragioni specifiche a sostegno della necessità di ricorrere a tale peculiare modalità di verifica dell'osservanza dell'orario di lavoro, peraltro già dichiarata sproporzionata dal Garante in precedenti casi analoghi (*cfr. Provv.* 21 luglio 2005 [doc. *web* n. 1150679]; nonché *Provv.* 15 giugno 2006 [doc. *web* n. 1306523, n. 1306530 e n. 1306551]). Inoltre, anche in questo caso, il sistema sarebbe stato impiegato per controllare l'osservanza dell'orario da parte dei soli dipendenti destinati ad accedere all'area riservata, con esclusione dei restanti lavoratori della società.

Il Garante ha infine prescritto alla società: a) di trattare, oltre ai dati biometrici relativi all'analisi delle impronte digitali, le sole informazioni necessarie al funzionamento del sistema biometrico (individuati nel codice identificativo individuale, nel codice assegnato al *badge* utilizzato quale supporto del *template* e nel profilo di autorizzazione); b) di indicare l'esistenza del sistema alternativo di identificazione nell'informativa agli interessati; c) di conservare i dati relativi agli orari di accesso alle aree riservate per il tempo massimo di sette giorni.

Impiego della geometria della mano per finalità di controllo accessi

Negli ultimi mesi dell'anno, una società consortile ha chiesto al Garante di sottoporre a verifica preliminare un sistema di riconoscimento biometrico con finalità di identificazione dei soggetti deputati ad accedere ad un complesso polifunzionale, sito in una zona ad alto rischio di criminalità e destinato ad ospitare oltre duecento esercizi artigianali e commerciali dedicati alla lavorazione e commercializzazione di materiali preziosi nel settore dell'oreficeria.

Il sistema ipotizzato si basava sull'impiego della geometria della mano (caratteristica biometrica il cui impiego non era stato ancora sottoposto al vaglio dell'Autorità), e ha richiesto l'esame congiunto di un sistema di controllo alternativo ipotizzato dalla società per consentire l'accesso ai soggetti che non avessero prestato il consenso al trattamento dei propri dati biometrici. Il sistema alternativo era costituito da impianti di videosorveglianza con una raccolta di immagini collegata, incrociata e/o confrontata con codici identificativi di carte elettroniche (in relazione all'eventuale opportunità che il titolare del trattamento si avvalga del procedimento di verifica preliminare anche in caso di utilizzo di impianti di videosorveglianza, *v.* il punto 3.2.1 del *Provv.* 29 aprile 2004 [doc. *web* n. 1003482]).

Dalle risultanze istruttorie è emerso che il sistema di verifica biometrica progettato dalla società, per la sola finalità di autorizzare l'accesso al complesso polifunzionale di soggetti operanti anche occasionalmente all'interno della struttura, sarebbe stato costituito da dispositivi di lettura della geometria della mano non centralizzati, integralmente autonomi nello svolgimento della procedura di identificazione biometrica, installati all'interno di bussole automatiche con porte interbloccate con accesso consentito ad una persona per volta.

La geometria della mano rilevata in occasione di ciascun ingresso al complesso polifunzionale sarebbe stata trasformata, mediante un *software* apposito, in un codice numerico associato all'interessato, da confrontare con un altro codice numerico ricavato dalla lettura della geometria della mano e già memorizzato su una *smart card* nell'esclusiva disponibilità dell'utente. L'accesso al complesso sarebbe avvenuto a seguito dell'associazione tra i due codici (preceduta dalla lettura della tessera di prossimità effettuata mediante i rilevatori) e della verifica di corrispondenza con altre informazioni (dati anagrafici, codice che associa la *smart card* all'utente, immagine del viso dell'interessato e profilo di autorizzazione individuale, ovvero fascia oraria e giorni consentiti per l'accesso) memorizzate in un *data-base* installato su un *server* protetto conformemente alle disposizioni del Codice e dell'Allegato B. al Codice medesimo.

Per i soggetti che non avessero prestato il consenso al trattamento dei propri dati biometrici, la società avrebbe previsto l'accesso alla struttura mediante un sistema alternativo basato sull'acquisizione dell'immagine del volto, associata ad un codice personale permanente (*pin*). L'accesso sarebbe avvenuto esclusivamente attraverso una delle bussole automatiche con porte interbloccate equipaggiate con telecamera e dispositivo a codice. Digitata l'esatta sequenza numerica sarebbero state visualizzate automaticamente, su apposito terminale dedicato, l'immagine video dell'utente intenzionato ad accedere, ripresa dalla menzionata telecamera e quella, relativa al volto, acquisita precedentemente assieme ai dati anagrafici e memorizzata su un *data-base* remoto. Un operatore appositamente incaricato avrebbe provveduto a confermare l'identità e ad autorizzare (o negare) l'accesso.

Il Garante (*Provv.* 1° febbraio 2007 [doc. *web* n. 1381983]) ha ritenuto conforme ai principi generali in materia di trattamento dei dati il sistema di rilevazione biometrica prospettato dalla società, alla quale è stato comunque prescritto di non apporre sulla *card* l'immagine dell'interessato e le indicazioni nominative, risultando sufficiente attribuire a ciascun interessato un codice individuale così da minimizzare, anche in caso di smarrimento, le possibilità di abuso delle informazioni memorizzate.

In relazione al sistema alternativo prefigurato si è ritenuto necessario prevedere la fornitura, agli interessati che non prestino il consenso al trattamento di dati biometrici, e unitamente al codice individuale, di un supporto sprovvisto di immagine dell'interessato, tenuto conto che l'identità di quest'ultimo può essere verificata agevolmente dal personale di vigilanza, confrontando l'immagine digitalizzata (raccolta in precedenza e memorizzata in una banca di dati dalla società) con quella ricavata mediante la telecamera posta nella bussola.

L'Autorità ha inoltre chiesto al titolare del trattamento di impartire agli interessati apposite istruzioni scritte alle quali attenersi, con particolare riguardo al caso di perdita o sottrazione delle *smart card*, nonché di indicare chiaramente, nell'informativa resa agli interessati in relazione alle immagini raccolte, l'esistenza di modalità alternative di accesso e di identificazione. Il Garante ha prescritto che i dati relativi agli accessi individuali al complesso polifunzionale siano conservati per il tempo massimo di sette giorni.

Linee-guida sul trattamento dei dati di lavoratori dipendenti di soggetti privati

Come si è già riportato, con il *provvedimento* 23 novembre 2006 (su cui *v.* più estesamente il *par.* 10.3.2), il Garante ha adottato "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", mettendo a disposizione dei datori di lavoro un quadro unitario di misure e accorgimenti conformi al Codice da tenere in considerazione nel trattamento di dati personali di lavoratori operanti alle loro dipendenze. In tale documento, con riguardo al trattamento di dati biometrici, preso atto del ricorso sempre più diffuso all'impiego di tali sistemi in ambito lavorativo, l'Autorità ha definito in termini generali alcune misure alle quali i titolari del trattamento devono attenersi, stabilendo che esse debbano essere oggetto di una prescrizione ai sensi degli artt. 17, 154, comma 1, lett. *c*), e 167, comma 2, del Codice, attesi i maggiori rischi specifici che tale trattamento comporta per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

Ove il trattamento di dati biometrici avvenga nei termini delineati dalle menzionate linee-guida, non è necessaria una valutazione preventiva dell'Autorità, mentre per fattispecie particolari non considerate nelle linee-guida medesime resta ferma la necessità della presentazione da parte del titolare del trattamento di apposito interpello ai sensi dell'art. 17 del Codice.

17.2. *L'utilizzo di credenziali biometriche nelle banche*

Sistemi di rilevazione di impronte digitali ed immagini per l'accesso a banche

A fronte della persistenza di fenomeni criminosi e del loro accentuarsi in alcune aree del Paese, alcuni istituti di credito, anche per il tramite dell'Abi-Associazione bancaria italiana, hanno rappresentato all'Autorità l'intenzione di avvalersi di sistemi di accesso più sicuri, attrezzando a tal fine i varchi d'accesso alle banche con videocamere e sistemi di rilevazione delle impronte digitali della clientela.

Nel solco dei principi già stabiliti dall'Autorità (*Provv.* 28 settembre 2001 [doc. *web* n. 39704]; *cfr. Relazione* 2001, p. 78), e con l'introduzione di garanzie ulteriori che hanno tenuto conto delle numerose segnalazioni pervenute, il Garante ha individuato le misure e gli accorgimenti cui tutti gli istituti di credito devono attenersi nel ricorso a tali dispositivi (*Provv.* 27 ottobre 2005 [doc. *web* n. 1246675], in *G.U.* 22 marzo 2006, n. 68; *v.* anche *Relazione* 2005, p. 69).

In particolare, con il provvedimento citato, adottato a seguito di una verifica preliminare ai sensi dell'art. 17 del Codice, l'Autorità ha ribadito l'illiceità dell'uso generalizzato di sistemi che associno immagini e impronte digitali, precisando che

possono essere trattati dati raccolti mediante la combinazione di telecamere e sistemi biometrici solo in presenza di condizioni di effettivo rischio e per l'esclusiva finalità di garantire un più elevato grado di sicurezza di beni e persone (tenendo conto, *ad es.*, della localizzazione dello sportello bancario: in luogo isolato, ovvero prossimo a vie di fuga, ovvero in aree interessate da precedenti rapine, *ecc.*).

Al fine di facilitare la richiesta di verifica preliminare da parte delle banche che installano i suddetti sistemi (e al contempo, per agevolare l'attività di controllo del Garante in tale settore), è stata predisposta una procedura che consente ai titolari del trattamento di inviare una comunicazione/richiesta di verifica preliminare per via telematica [doc. *web* n. 1243256 e n. 1247352]. Al 20 febbraio 2007, le agenzie presso le quali sono stati attivati tali sistemi sono risultate oltre duemila.

Nel provvedimento citato sono state, altresì, prescritte specifiche misure a garanzia degli interessati. In particolare, oltre all'informativa comprensiva degli elementi previsti dall'art. 13 del Codice, sono stati fissati i tempi di conservazione dei dati raccolti, per un periodo massimo di una settimana, e sono state previste modalità di accesso alternativo alle agenzie ove il cliente non intenda o non possa prestarsi a simili operazioni di trattamento. I sistemi di videosorveglianza devono riprendere esclusivamente l'accesso all'istituto di credito; può essere rilevata solo l'impronta dattiloscopica dell'interessato.

In alcuni casi portati all'attenzione del Garante, il ricorso a dati biometrici ricavati dalle impronte digitali ha formato oggetto di verifiche preliminari in relazione a trattamenti finalizzati a rendere particolari servizi alla clientela o a limitare l'accesso in "aree sensibili" degli istituti di credito.

Filiale *high tech*

A tale proposito, vanno segnalate due decisioni adottate dall'Autorità, la prima delle quali ha preceduto l'attuazione di un progetto sperimentale denominato "Filiale *high tech*", in base al quale i clienti possono essere dotati a richiesta di una *smart card* con microprocessore *Rfid* per facilitare la fruizione di taluni servizi, rendendo immediatamente visibile la propria "posizione" sul terminale del personale operante presso la banca. Inoltre, i dati biometrici memorizzati sulla medesima *smart card*, a seguito del procedimento di autenticazione e di identificazione, consentono alla clientela un accesso più agevole a talune aree dedicate.

Alla luce dell'attività istruttoria svolta il Garante non ha rilevato profili di illiceità nel trattamento indicato, ma ha stabilito misure e accorgimenti ai quali la banca deve attenersi al fine di garantire la conformità del trattamento ai principi di protezione dei dati personali (*Provv.* 23 febbraio 2006 [doc. *web* n. 1251535]). In particolare:

- è stata considerata sproporzionata la centralizzazione in un *data-base* delle informazioni personali relative ai clienti che richiedono di disporre dei servizi offerti dalla "filiale *high tech*" ed è stata consentita, in luogo di essa, una procedura di verifica basata sul confronto tra le impronte rilevate ad ogni accesso al sistema e il modello memorizzato e cifrato su un supporto posto nell'esclusiva disponibilità degli interessati;
- è stata disposta l'adozione di misure idonee affinché, in caso di smarrimento o furto, vengano immediatamente inibite, in modo automatico, tutte le funzioni connesse all'uso della *service card*.

Accesso ad aree sensibili

Un secondo caso ha riguardato la richiesta di un istituto di credito di sottoporre a verifica preliminare il trattamento di dati biometrici ricavati dalle impronte digitali per accedere a particolari locali della propria sede non aperti al pubblico (in particolare, la sala del consiglio di amministrazione, gli uffici di presidenza, la direzione generale e la segreteria generale). Con tale sistema, la banca intendeva incrementare la sicurezza personale di coloro che lavorano nelle aree menzionate e assicurare una protezione più elevata alla documentazione e ai beni ivi custoditi. Il sistema sarebbe

stato costituito da lettori di impronta digitale situati negli ascensori che portano ai piani indicati, tramite i quali il modello dell'impronta rilevata sarebbe stata confrontata con quella registrata in un *data-base* centralizzato della banca.

Il trattamento di dati oggetto di verifica preliminare è stato ritenuto lecito alla luce delle specifiche finalità perseguite nel contesto esaminato e delle misure prescritte dal Garante, che ha tuttavia ribadito la sproporzione e non necessità della centralizzazione in un archivio dei dati biometrici, anche alla luce del principio di minimizzazione dell'utilizzo di dati personali nei sistemi informativi (art. 3 del Codice).

L'Autorità ha quindi prescritto alla società di predisporre un sistema di riconoscimento basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il *template*, memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità degli interessati (*Provv.* 15 giugno 2006 [doc. *web* n. 1306098]).

17.3. *Videosorveglianza e sistemi biometrici in ambito pubblico*

Come negli anni passati, anche nel 2006 sono pervenuti numerosi quesiti e segnalazioni aventi ad oggetto le tematiche relative all'installazione e all'utilizzo da parte di amministrazioni pubbliche di sistemi di videosorveglianza. In proposito sono state ribadite volta per volta le indicazioni per un corretto utilizzo di telecamere da parte di soggetti pubblici in specifici settori, sottolineando le prescrizioni già a suo tempo fornite con il *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482].

Videosorveglianza nelle scuole

In particolare, in ambito scolastico, il Garante ha precisato che il Codice è applicabile in relazione ai trattamenti effettuati attraverso sistemi di videosorveglianza, anche se le immagini sono utilizzate solo nel quadro di un circuito chiuso e non sono soggette a registrazione. È stato ribadito che l'installazione di telecamere in una scuola può essere giustificata solo se strettamente indispensabile, come *ad es.* in caso di ripetuti atti vandalici o fuori dell'orario scolastico, quando gli edifici sono chiusi (*Note* 5 luglio 2006 e 20 luglio 2006).

Videosorveglianza in Asl e ambulatori

La necessità di una specifica attenzione al principio generale di proporzionalità tra i mezzi impiegati e le finalità perseguite è stata richiamata in relazione alla richiesta, pervenuta da un'azienda sanitaria, di poter utilizzare una telecamera a circuito chiuso da installare nei servizi igienici dell'utenza, al fine di garantire l'autenticità dei controlli tossicologici svolti dalla stessa azienda.

L'Autorità, 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, ancorché a circuito chiuso, nei servizi igienici di una Asl, al fine di evitare che la raccolta delle urine possa essere oggetto di falsificazione, lungi dal costituire una misura a tutela della *privacy* dell'interessato, può configurarsi al contrario come eccessivamente lesiva della sua dignità. L'Autorità ha richiamato in merito le vigenti norme in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga protezione (*toilette*, stanze d'albergo, cabine, spogliatoi, *ecc.*) (*Nota* 19 ottobre 2006).

A seguito dell'invito rivolto all'azienda sanitaria ad indicare le ragioni che avrebbero reso indispensabile, per le finalità sopra indicate, l'installazione di sistemi di videosorveglianza nei servizi igienici destinati all'utenza, in luogo di altri sistemi o procedure meno pericolosi o rischiosi per i diritti e le libertà fondamentali degli interessati, l'azienda stessa ha rivalutato l'esigenza rappresentata al Garante.

Sono state, inoltre, nuovamente sottolineate le cautele previste nel provvedi-

17

mento generale per l'installazione di telecamere presso ambulatori medici. In particolare, a seguito di una segnalazione, è stato rappresentato ad un ambulatorio –che aveva attivato telecamere all'interno degli spogliatoi e anche durante le visite mediche– che 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 che deve essere adottato ogni ulteriore accorgimento necessario a garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate (*cfr.* anche *Provv.* 9 novembre 2005 [doc. *web* n. 1191411]).

Nel richiamare l'attenzione sulla particolare delicatezza del trattamento ipotizzato, in ragione della natura delle informazioni impiegate, l'ambulatorio è stato invitato ad informare l'Autorità in ordine alle iniziative assunte al fine di rendere il trattamento dei dati conforme al quadro di garanzie delineato nei citati provvedimenti generali. Sul riscontro fornito sono in corso accertamenti (*Nota* 18 settembre 2006).

Abbandono di rifiuti

L'Autorità è stata poi nuovamente interpellata in ordine all'utilizzo di sistemi di videosorveglianza al fine di prevenire, limitare ed eventualmente perseguire comportamenti illeciti in ambito ambientale, specie con riferimento all'abbandono di rifiuti. Tale utilizzo è considerato lecito solo se risultano inefficaci o inattuabili altre misure; al contrario, un controllo video, effettuato al solo scopo di accertare infrazioni amministrative rispetto a disposizioni concernenti le modalità e l'orario di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori, non risulta lecito (*Nota* 19 ottobre 2006).

Richieste irrituali di "verifica preliminare"

In numerosi casi, sono stati trasmessi al Garante dai soggetti pubblici "regolamenti in materia di videosorveglianza", con la contestuale richiesta di "verifica preliminare" ovvero di "autorizzazione".

Al riguardo, si è fatto presente ripetutamente che il citato provvedimento generale del 29 aprile 2004 individua espressamente le ipotesi in cui i titolari del trattamento sono tenuti a sottoporre alla verifica preliminare, ad autorizzazione e a notificazione al Garante i sistemi di videosorveglianza che intendono attivare (*Note* 16 giugno 2006, 5 luglio 2006, 25 luglio 2006, 22 settembre 2006, 26 settembre 2006, 23 ottobre 2006, 3 novembre 2006 e 5 gennaio 2007). Spetta all'amministrazione richiedente valutare se i trattamenti di dati personali effettuati nell'ambito di un'attività di videosorveglianza siano riconducibili alle ipotesi previste nel provvedimento generale. Il Garante ha infatti richiesto che siano sottoposti alla verifica preliminare i soli sistemi di videosorveglianza che danno luogo ad una raccolta delle immagini collegata, incrociata o confrontata con altri particolari dati personali (*ad es.*, dati biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce.

La verifica preliminare del Garante è inoltre prevista in caso di digitalizzazione o indicizzazione delle immagini (che rendano possibile una ricerca automatizzata o nominativa) o di videosorveglianza *cd.* "dinamico-preventiva" che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (*ad es.*, mediante sistemi di riconoscimento facciale) o eventi improvvisi, o comportamenti anche non previamente classificati.

Fuori dai predetti casi, i trattamenti di dati mediante sistemi di videosorveglianza non devono essere sottoposti all'esame preventivo del Garante. È stato pertanto ribadito a diverse amministrazioni che non può desumersi alcuna approvazione implicita dalla mera trasmissione all'Autorità di comunicazioni o progetti relativi alla intenzione di installare sistemi di videosorveglianza. Non è infatti stabilito alcun termine decorso il quale i progetti sottoposti alla verifica del Garante possano ritenersi dalla stessa autorizzati, anche perché in merito non trova opportunamente applicazione il principio del silenzio-assenso.

Sono inoltre pervenute numerose segnalazioni, nonché specifiche richieste di parere da parte di amministrazioni pubbliche, in merito all'utilizzo di sistemi di rilevazione automatica delle presenze mediante il riconoscimento delle impronte digitali. L'Autorità ha così avviato diverse istruttorie, attualmente in corso di svolgimento, in merito alla liceità dell'utilizzo di tali sistemi per il controllo dell'accesso al luogo di lavoro da parte dei dipendenti.

Utilizzo di dati biometrici nel settore pubblico

17.4. *Il decalogo su corpo e* privacy

Intervenendo il 9 maggio 2006 al *ForumPa* nel convegno su *"Le nuove tecnologie per la gestione dell'identità: l'utilizzo dei dati biometrici"*, il componente del Collegio Giuseppe Fortunato ha sottolineato l'inderogabile esigenza di rispettare il corpo umano nell'utilizzo delle nuove tecnologie e nella rilevazione dei dati biometrici.

A tal fine ha illustrato, sulla base dei provvedimenti adottati dal Garante in varie fattispecie, un "decalogo" sull'uso del corpo, articolato in dieci punti, che affronta i temi dell'affidabilità del sistema di rilevazione, dell'informativa e del consenso dell'interessato, dei principi di liceità e necessità del trattamento, della conservazione temporanea dei dati, delle misure di sicurezza idonee ad evitare la possibilità indiscriminata di decifrare le informazioni acquisite, della piena conoscibilità dei dati biometrici da parte dell'interessato, del rispetto rigoroso degli obblighi di verifica preliminare e di notifica al Garante, della necessità di prevedere la disattivazione automatica immediata e certa di funzioni di *smart card* o altre analoghe nel caso di smarrimento o di furto [doc. *web* n. 1277433].