15 - La videosorveglianza e la biometria

[doc. web n. 1638180]

15. La videosorveglianza e la biometria [72 Kb.]

15.1. Videosorveglianza in ambito pubblico

Anche nel 2008 l´Autorità è stata chiamata a fornire indicazioni sull´applicazione del *provvedimento* generale in materia di videosorveglianza del 29 aprile 2004 (doc. *web* n. 1003482).

Più volte è stata richiamata l´attenzione sulle garanzie da osservare nell´ambito dei rapporti di lavoro anche quando gli impianti siano utilizzati per esigenze organizzative e dei processi produttivi, ovvero siano richiesti per la sicurezza del lavoro (punto 4.1 del *cit. provvedimento* generale) (*Note* 3 marzo 2008, 13 marzo 2008, 30 aprile 2008, 2 settembre 2008, 24 novembre 2008 e 9 gennaio 2009).

Ad un ente locale che aveva installato impianti di videosorveglianza attraverso web cam, diffondendo le immagini in tempo reale sul suo sito istituzionale, è stato fatto presente che non risulta di regola giustificata un´attività di sorveglianza rivolta non al controllo di eventi, situazioni e avvenimenti, ma a fini promozionali-turistici o pubblicitari, attraverso *web cam* o *cameras-on-line* che consentano di individuare i tratti somatici delle persone che figurano nei campi visuali ripresi, rendendole identificabili (*cfr*. punto 2.3 del citato provvedimento e *Provv*. 14 giugno 2001 [doc. *web* n. 41782]) (*Nota* 15 maggio 2008).

Nel corso di un accertamento ispettivo disposto dal Garante su segnalazione era emerso che delle cinque telecamere installate presso uno studio medico, due riprendevano le immagini dell´ingresso ai locali e tre erano posizionate all´interno dei luoghi destinati a spogliatoio. Alla luce delle vigenti disposizioni in tema di interferenze illecite nella vita privata, di tutela della dignità, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (*Provv*. 29 aprile 2004, punto 2.1.), il trattamento svolto attraverso l´installazione di telecamere negli spogliatoi non è risultato effettuato in modo lecito.

In particolare, è stato valutato che la collocazione di telecamere operanti in modo continuo negli spogliatoi di un ambulatorio medico determina un´intromissione ingiustificata nella vita privata delle persone che vi si recano risultando, pertanto, essere lesiva della loro riservatezza e dignità. Sono stati conseguentemente vietati all´ambulatorio, ai sensi dell´art. 154, comma 1, lett. *d*), del Codice, ulteriori trattamenti illeciti aventi per oggetto i dati personali raccolti mediante il descritto

sistema di videosorveglianza installato negli spogliatoi (*Provv*. 4 dicembre 2008 [doc. *web* n. 1576125]).

Ad un´azienda sanitaria locale, che aveva formulato un quesito sull´installazione di un sistema di videosorveglianza presso alcune sedi operative dei Servizi per le tossicodipendenze dislocate sul territorio provinciale, è stato fatto presente che il sistema avrebbe potuto evidenziare anche profili inerenti le condizioni di salute dei pazienti. Pertanto, 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 rendendo accessibili le immagini unicamente ai soggetti specificamente autorizzati (*ad es*., personale medico ed infermieristico).

Nei casi in cui l´impiego di un sistema di videosorveglianza degli accessi sia utilizzato a salvaguardia del patrimonio aziendale e per monitorare le zone nevralgiche e a rischio per la sicurezza dei pazienti e dei visitatori, dati idonei a rilevare lo stato di salute, l´appartenenza etnica o razziale e le convinzioni religiose possono essere rilevati incidentalmente anche attraverso la ripresa dei tratti somatici o dell´abbigliamento degli interessati o il contesto in cui è effettuata la ripresa (v. art. 20, comma 2, del Codice; scheda n. 41 dell´Allegato B.; schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari di competenza delle regioni, delle province autonome, delle aziende sanitarie, degli enti regionali/provinciali e degli enti vigilati e controllati dalle regioni e dalle province autonome, sul quale, in data 13 aprile 2006, l´Autorità ha espresso parere favorevole [doc. *web* n. 1272225]; punto 4.2 del *cit. Provv.* 29 aprile 2004) (*Nota* 30 gennaio 2009).

Da ultimo, si menziona la segnalazione di un nucleo operativo dei Carabinieri di una regione, relativa al trattamento di dati effettuato da taluni comuni con apparecchiature elettroniche per il rilevamento automatico di infrazioni al codice della strada. In particolare, si lamentava la mancata designazione, quali responsabili ed incaricati del trattamento, dei soggetti coinvolti nell´installazione e nel funzionamento delle apparecchiature in questione.

Sulla base degli elementi ottenuti dai comuni, in un caso l´Ufficio ha evidenziato, in particolare, che il titolare del trattamento deve specificare analiticamente e per iscritto i compiti affidati al responsabile, con particolare riferimento al trattamento dei dati personali, ed è tenuto a vigilare sul rispetto delle vigenti disposizioni, ivi compreso il profilo relativo alla sicurezza, anche tramite verifiche periodiche (art. 29, commi 4 e 5, del Codice). In mancanza di tali designazioni, la trasmissione di dati personali da parte di soggetti pubblici a soggetti esterni privati si configura come una comunicazione ed è, in quanto tale, assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice) (*Note* 26 maggio 2008, 24 luglio 2008 e 28 luglio 2008).

Videosorveglianza a bordo taxi

A seguito di notizie di stampa – che evidenziavano l´installazione di sistemi di videosorveglianza all´interno delle autovetture adibite al servizio taxi, in attuazione di progetti pubblici volti a promuovere la sicurezza nell´ambito del menzionato servizio – l´Autorità ha richiesto informazioni ad alcune compagnie/cooperative di radio-taxi per valutare la liceità dei trattamenti. Solo due compagnie hanno dichiarato di avere in corso l´installazione (in via di completamento entro la fine del 2008) di un sistema di videosorveglianza dotato di minicamera a infrarossi e relativa interfaccia di acquisizione delle foto (denominata *"black box"*). La menzionata minicamera scatterebbe fotografie ai clienti memorizzate nella black box in formato criptato (destinate ad essere sovrascritte dopo circa 24 ore dalla loro acquisizione); solo in caso di allarme lanciato dal tassista (*ad es.*, in caso di aggressione) le immagini raccolte a partire dai dieci minuti antecedenti l´allarme verrebbero trasmesse dal sistema

mediante protocollo radio non accessibile a terzi (oltre a poter essere *"scaricate"* direttamente dalla *black box*) e rese fruibili a un incaricato della centrale *radio-taxi* dotato di *chip card* di autenticazione per consentire di contattare le autorità di polizia. L´impianto, predisposto nel rispetto del principio di necessità (verrebbero rese utilizzabili le sole foto scattate nei dieci minuti antecedenti alla sua attivazione, in caso di emergenza, da parte del tassista), sarebbe altresì provvisto di accorgimenti *hardware* e *software* ritenuti in grado di rendere inaccessibile i dati a tassisti, installatori, e ad altri soggetti non autorizzati; solo la compagnia/cooperativa potrebbe accedere ai dati registrati in caso di richiesta delle informazioni da parte delle forze dell´ordine (debitamente autorizzate dall´autorità giudiziaria). Il sistema di videosorveglianza e il conseguente trattamento dei dati personali verrebbe segnalato alla clientela mediante apposita vetrofania, visibile anche all´esterno del veicolo raffigurante l´icona della telecamera conforme a quella presente sul sito dell´Autorità. Sono in corso gli opportuni approfondimenti sulla liceità del trattamento.

152 Biometria in ambito pubblico

Nel corso dell´anno numerose richieste hanno evidenziato l´interesse dei soggetti pubblici per i sistemi di rilevazione automatica per il controllo degli accessi al luogo di lavoro mediante il riconoscimento dei dati biometrici dei dipendenti. Si è reso necessario, quindi, ribadire le indicazioni contenute nel provvedimento generale recante *"Linee-guida in materia di 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 cinquantaquattro casi sono pervenute richieste di verifica preliminare relative all´utilizzo di dati biometrici; nella quasi totalità di essi non era richiesta tale procedura, prevista nel Codice all´art. 17, con riferimento ai trattamenti di dati personali – diversi da quelli sensibili e giudiziari – che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell´interessato.

Due richieste sono state definite con *provvedimento* favorevole (Azienda Policlinico Umberto I, *Provv*. 15 aprile 2008 [doc. *web* n. 1523435]; Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa (*Provv*. 19 giugno 2008 [doc. *web* n. 1532480]) mentre altre tre sono ancora all´esame del Collegio in ragione della particolare delicatezza dei casi sottoposti, che ha reso necessario un supplemento di istruttoria.

Per quanto riguarda l´Azienda Policlinico Umberto I, la richiesta era incentrata sull´installazione di lettori biometrici per: 1) permettere l´accesso a locali ed aree a rischio; 2) autenticazione informatica; 3) verificare la presenza del personale in servizio. Al riguardo, il Garante ha fornito prescrizioni e accorgimenti nei primi due casi, non ritenendo invece proporzionato l´utilizzo di tecniche biometriche nel terzo.

L´Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa aveva invece avanzato richiesta di verifica preliminare per la raccolta di dati biometrici, desunti dall´impronta digitale, di pazienti e personale sanitario da associare alle sacche di sangue destinate alla trasfusione, per prevenire errori dei identificazione di pazienti o delle unità di sangue in sede di trasfusione, fonti di conseguenze gravissime. Il provvedimento favorevole del Garante ritiene proporzionata allo scopo la modalità del trattamento prospettata dall´Azienda, ed indica alcuni accorgimenti da adottare, in particolare per quanto attiene alla conservazione dei dati.

In più occasioni, il Garante ha ricordato 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; ha fatto altresì presente che 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 (*Note* 24 giugno 2008, 3 settembre 2008, 14 novembre 2008 e 11 dicembre 2008).

In due occasioni il Garante ha precisato che, di regola, tali sistemi possono essere attivati soltanto per particolari esigenze di controllo dell´accesso a speciali aree dei luoghi di lavoro ad esempio, perché l´aerea è destinata allo svolgimento di attività aventi carattere di segretezza, ovvero che comportano la necessità di trattare informazioni rigorosamente riservate (ad es., accesso a sale operative ove confluiscono segnalazioni afferenti alla sicurezza anticrimine; aree adibite ad attività inerenti alla difesa e alla sicurezza dello Stato; ambienti di torri di controllo aeroportuali), nonché alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere circoscritta in quanto un utilizzo improprio può determinare un rischio grave e concreto per la salute e l´incolumità dei dipendenti o di terzi (ad es., ambienti ove sono custodite sostanze stupefacenti o psicotrope) (*Note* 17 ottobre 2008, 30 gennaio 2009 e 13 febbraio 2009).

Nelle medesime occasioni è stato altresì ricordato che il trattamento di dati relativi alle impronte digitali è ammesso a condizione che sia sottoposto con esito positivo – di regola a seguito di un interpello del titolare – alla verifica preliminare prevista dall´art. 17 del Codice anche per determinate categorie di titolari o di trattamenti; che venga effettuata preventivamente la notificazione al Garante (artt. 37, comma 1, lett. *a*) e 38 del Codice); che non sia comunque registrata l´immagine integrale dell´impronta digitale, bensì solo il modello di riferimento da essa ricavato (template); che tale modello non sia archiviato in una memoria centralizzata, bensì in un supporto posto nell´esclusiva disponibilità dell´interessato (*smart card* o dispositivo analogo) e privo di indicazioni nominative riferibili a quest´ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale); che sia fornita ai dipendenti interessati un´informativa specifica per il trattamento in questione (art. 13 del Codice).

Ad una agenzia per il diritto allo studio universitario è stato fatto presente che la raccolta e la registrazione di impronte digitali e dei codici numerici da esse ricavati, e successivamente utilizzati per effettuare il confronto tra il *"modello"* di impronta digitale memorizzato nel microchip del tesserino rilasciato allo studente e quello di volta in volta elaborato dal programma di gestione sulla base della rilevazione dell´impronta digitale, sono operazioni di trattamento di dati personali riconducibili ai singoli interessati (art. 4, comma 1, lett. *b*), del Codice). Pertanto, trovando applicazione la normativa contenuta nel Codice, il trattamento con tali modalità volto al controllo degli accessi alla mensa universitaria non sarebbe risultato, allo stato degli atti, effettuato in modo lecito (*Nota* 1° dicembre 2008).

153 Videosorveglianza in ambito privato

Salvo quanto si dirà di seguito sui trattamenti effettuati in ambito condominiale mediante sistemi di videosorveglianza, deve rilevarsi che la materia continua a formare oggetto di numerose segnalazioni (esaminate alla luce della legge e del *provvedimento* generale del 29 aprile 2004 [doc. web n. 1003482]), come pure di controlli da parte dell´Autorità, spesso con l´ausilio della Guardia di finanza. Peraltro, la disciplina di protezione dei dati personali non trova applicazione, ai sensi dell´art. 5, comma 3, del Codice, in caso di trattamenti di dati per fini esclusivamente personali – e i rapporti di vicinato rientrano per lo più in quest´ambito – salvo che le immagini registrate non siano oggetto di comunicazione sistematica o diffusione. In tal caso, sussistendone i presupposti, l´interessato può far valere i propri diritti avanti all´autorità giudiziaria ordinaria, anche a mente del divieto sanzionato penalmente relativo all´indebita raccolta (mediante l´uso di strumenti di ripresa visiva o sonora, nonché alla rivelazione e alla diffusione) di immagini attinenti alla vita privata che si svolgono nell´abitazione altrui o in un altro luogo di privata dimora (art. 615-*bis* c.p. - Interferenze illecite nella vita privata).

Videosorveglianza e condominio

A seguito di alcuni quesiti e segnalazioni è stata inviata una segnalazione al Parlamento e al Governo sull´eventualità di disciplinare con norme apposite alcuni profili relativi alla videosorveglianza all´interno di edifici condominiali e nelle relative pertinenze. Tale tematica, con particolare riferimento alle condizioni di liceità del trattamento, ai soggetti deputati a manifestare la volontà per svolgerlo e alle eventuali maggioranze da rispettare, non è stata oggetto di valutazione specifica nei due provvedimenti di carattere generale adottati in materia di videosorveglianza (*Provv*. 29 novembre 2000 [doc. *web* n. 31019], 29 aprile 2004 [doc. *web* n. 1003482]).

Al riguardo, è emersa l´esistenza di due contrapposti interessi: da un lato, l´esigenza di preservare la sicurezza di persone e la tutela di beni comuni; dall´altro, la preoccupazione che, nel rendere più agevolmente conoscibili a terzi abitudini e stili di vita individuali e familiari, si incida sulla libertà degli interessati di muoversi, non controllati, nel proprio domicilio e all´interno delle aree condominiali.

Considerato che il profilo in esame non trova regolamentazione specifica e che gli orientamenti giurisprudenziali sull´utilizzo delle aree comuni non appaiono sufficienti a dissolvere tutti i dubbi al medesimo relativi, l´Autorità, anche alla luce di quanto previsto dalla disciplina penalistica in tema di interferenze illecite nella vita privata, ha auspicato un eventuale intervento normativo chiarificatore (anche nell´ambito di alcuni più ampi disegni di legge già oggetto di attenzione da parte di entrambi i rami del Parlamento) per un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di difesa e protezione di persone e cose (Segnalazione al Parlamento e al Governo 13 maggio 2008 [doc. *web* n. 1523997]).

Esercizi commerciali e videosorveglianza

Sono pervenute due distinte segnalazioni relative all´installazione, presso un esercizio commerciale, di un sistema di videosorveglianza in asserita violazione della disciplina di protezione dei dati personali. Dall´istruttoria (anche con accertamenti in loco) è risultato che il titolare del trattamento non ha designato il soggetto incaricato di mantenere l´impianto quale responsabile del trattamento (art. 29 del Codice), ancorché unico soggetto autorizzato ad accedere alle immagini registrate; ciò ha configurato la possibilità di una comunicazione a terzi (ai sensi dell´art. 4, comma 1, lett. *l*), del Codice) da parte del medesimo titolare del trattamento in assenza del consenso informato degli interessati (artt. 13 e 23 del Codice) o di un altro presupposto equipollente di liceità (art. 24 del medesimo Codice). In proposito, il Garante ha prescritto di designare il manutentore del sistema quale responsabile del trattamento, disponendo nelle more il blocco della comunicazione a tale soggetto delle immagini registrate. È inoltre emerso che il sistema consente la registrazione audio della voce degli interessati. Al riguardo – a prescindere da eventuali profili di liceità penale (artt. 617, 617-*bis* e 623-*bis* c.p.) – l´Autorità ha vietato l´ulteriore trattamento della voce degli interessati, in assenza di idonei e comprovati elementi giustificativi, in quanto effettuato in violazione del principio di finalità (secondo cui il trattamento deve essere effettuato per finalità determinate, esplicite e legittime – art. 11, comma 1, lett. *b*), del Codice – che non sono risultate ricorrere nella fattispecie) (*Provv*. 2 ottobre 2008 [doc. *web* n. 1581352]).

Videosorveglianza e difesa in giudizio

In un reclamo è stata contestata l´installazione in aree condominiali di un sistema di videosorveglianza (e la successiva produzione in giudizio di immagini riferite al reclamante acquisite attraverso il menzionato sistema) da parte di uno studio di consulenza avente sede nel condominio. Dagli elementi acquisiti è risultato che l´impianto era stato installato dallo studio (in passato oggetto di atti vandalici e intimidatori) per finalità di sicurezza dei propri beni patrimoniali e di deterrenza. Tale impianto (peraltro disattivato all´epoca della richiesta di informazioni) aveva in passato consentito di acquisire in ordine all´autore dei predetti atti (individuato nel medesimo reclamante) informazioni successivamente depositate presso la competente autorità giudiziaria nell´ambito di un procedimento penale al riguardo instaurato. Tenuto conto che le immagini (fatte salve quelle depositate presso la procura) non sono state conservate dal titolare e che sull´utilizzabilità di quelle prodotte in giudizio ogni valutazione spetta all´autorità giudiziaria (artt. 47 e 160, comma 6, del Codice), non sono stati ravvisati i presupposti per un intervento da parte dell´Autorità (art. 11, comma 1, lett. *b*), reg. Garante 1/2007). Nondimeno, l´Autorità ha richiamato il titolare del trattamento, in caso di eventuale riattivazione del sistema, al rispetto dei princìpi evidenziati nel *provvedimento* del 29 aprile 2004 (con specifico riferimento all´angolo visuale di ripresa) (*Nota* del 16 aprile 2008).

154 Biometria in ambito privato

Trattamenti di dati biometrici per finalità di rilevazione della presenza dei lavoratori

Alcuni accertamenti ispettivi svolti tramite la Guardia di finanza hanno evidenziato l´esistenza presso due società di sistemi di rilevazione dei dati biometrici per accertare la presenza dei dipendenti sui luoghi di lavoro.
In termini generali, l´utilizzo di dati biometrici nel contesto lavorativo può risultare giustificato solo per presidiare accessi ad *"aree sensibili"* (in ragione delle attività ivi svolte) (cfr. *Provv*. 21 luglio 2005 [doc. *web* n. 1150679]; *"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"* [doc. web n. 1364939]), non per finalità connesse all´ordinaria gestione del rapporto di lavoro.
Le società sono state perciò invitate a fornire riscontro sulle misure volte ad adeguare il trattamento dei dati biometrici riferiti ai lavoratori ai princìpi richiamati nei menzionati provvedimenti.

La prima società ha precisato di aver installato in sostituzione del pregresso sistema biometrico (per le finalità di gestione delle presenze e degli orari del personale in servizio) appositi *badge* per la timbratura del cartellino elettronico (cfr. *Nota* del 30 ottobre 2008).
La seconda ha dichiarato di essersi adoperata, per installare un nuovo sistema di rilevazione delle presenze in sostituzione del precedente che rilevava i dati biometrici dei dipendenti.

Tenuto conto delle affermazioni rese dalla società (secondo cui il sistema installato risulterebbe idoneo ad essere configurato come un normale terminale di rilevazione delle presenze in grado di leggere i *badge* passivi di prossimità), non è stata promossa l´adozione di un provvedimento da parte dell´Autorità (cfr. *Nota* del 18 novembre 2008). La società ha peraltro fatto successivamente

sapere di essersi dotata di un sistema *"tradizionale"* di rilevazione delle presenze dei lavoratori.

Dati biometrici e garanzie dei lavoratori

Sono pervenute anche nel 2008 alcune richieste di verifica preliminare sul trattamento di dati personali biometrici dei dipendenti. In un caso la richiesta era stata avanzata da una fondazione bancaria con sede in un immobile di alto valore artistico con più accessi, che renderebbero possibile a estranei di introdursi all´interno del palazzo senza essere visti. La finalità perseguita, consistente nell´assicurare la sicurezza di un immobile di elevato valore (anche per le opere d´arte in esso contenute) è risultata lecita, anche alla luce delle linee-guida sul trattamento di dati personali per la gestione del rapporto di lavoro (*Provv*. 23 novembre 2006 [doc. *web* n. 1364099]). Nel fornire, pertanto, alcune indicazioni affinché il trattamento fosse conforme alla disciplina di protezione dei dati personali, non si è ritenuto necessario un *provvedimento ad hoc* (*Nota* 18 aprile 2008).

L´adozione di un *provvedimento* è, invece risultata opportuna a seguito di una richiesta, avanzata da una società che gestisce servizi idrici, per trattare i dati biometrici dei dipendenti al fine di controllarne gli accessi a impianti di potabilizzazione e alle sedi centrale e periferiche della società. Il sistema, che prevede il consenso dei dipendenti, si basa su una raccolta di dati biometrici mediante apparecchiature dotate di lettore di impronte digitali e di un apposito *software*; l´impronta digitale verrebbe trasformata in un codice numerico (*template*), memorizzato su *smart card* e utilizzato esclusivamente per la raccolta e il successivo trattamento dei dati ai fini predetti. A livello centralizzato verrebbero memorizzati per sette giorni i dati personali relativi all´orario degli accessi giornalieri e i codici numerici che consentono alla società di risalire al dipendente.

Il trattamento è stato ritenuto lecito, tenendo conto della finalità di incrementare la sicurezza dell´impianto idrico anche con misure preventive a tutela della qualità delle acque (peraltro oggetto del d.lg. 2 febbraio 2001, n. 31, recante *"Attuazione della Direttiva 98/83/Ce relativa alla qualità delle acque destinate al consumo umano"*) e di assicurare così, mediatamente, la salute pubblica.

Si è, tuttavia, ravvisata l´esigenza di trattare i dati biometrici solo dei lavoratori per i quali, a seguito di una ricognizione preventiva, la società constati e documenti l´effettiva necessità di accedere alle aree meritevoli di protezione. A tal fine, il meccanismo da utilizzare deve essere basato sulla lettura delle impronte digitali cifrate su uno strumento disponibile per il lavoratore (*smart card* o analoghi dispositivi), senza creare un archivio centralizzato dei *template* derivati dall´analisi delle impronte digitali. Il Garante ha comunque rappresentato la necessità del previo assolvimento degli obblighi previsti dall´art. 4 dello Statuto dei lavoratori (*Provv*. 15 febbraio 2008 [doc. *web* n. 1497675]).

Biometria e luoghi di lavoro

L´Autorità ha vietato ad una società, perché illegittimo e invasivo, l´ulteriore trattamento dei dati raccolti attraverso un sistema di rilevazione di dati biometrici ricavati dalle impronte digitali installato in alcune sedi di lavoro solo per commisurare la retribuzione agli orari di lavoro effettivi. Nel caso (segnalato da uno dei dipendenti interessati) non sono, infatti, emerse ragioni concrete e specifiche in grado di giustificare l´utilizzo di dati biometrici. Il trattamento non è risultato conforme neanche alle indicazioni in materia contenute nelle *"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"* (*Provv*. 23 novembre 2006 [doc. *web* n. 1364099]). Inoltre, non

era stata rispettata la procedura prescritta dall´art. 4 della legge n. 300/1970, da osservare (*cfr.* Cass. 17 luglio 2007, n. 15892) nel caso in cui le apparecchiature consentano di controllare il rispetto degli orari di entrata e uscita e la presenza sul luogo di lavoro da parte dei dipendenti (*Provv*. 2 ottobre 2008 [doc. *web* n. 1571502]).

In un altro caso, all´esito di verifiche, anche ispettive, presso una società di trasporti campana, il trattamento di dati biometrici è risultato svolto in termini non compatibili con le suddette linee-guida del 23 novembre 2006 [doc. *web* n. 1364099]. La società, invitata ad attenersi al rispetto di tali prescrizioni, ha ritenuto eccessivamente onerosi gli investimenti a tal fine necessari, comunicando all´Autorità la dismissione degli apparati di rilevazione biometrica sperimentalmente installati. Essa è stata, in ogni caso, richiamata all´osservanza di quanto prescritto dagli articoli 16, comma 1, e 38, comma 4, del Codice per la cessazione del trattamento dei dati biometrici dei lavoratori (*Nota* 11 dicembre 2008).

Riconoscimento vocale e credenziali di autenticazione

A seguito di un´istanza di verifica preliminare ai sensi dell´art. 17 del Codice, il Garante ha autorizzato, per l´autenticazione degli accessi ai sistemi informativi di una società, il trattamento di dati personali dei dipendenti della società medesima, basato sul riconoscimento dei dati biometrici degli interessati. Il sistema si basa sulle impronte vocali criptate in forma di modello algoritmico, con l´ausilio di una società esterna (che memorizzerebbe alcune informazioni personali degli utenti su un proprio *server*) e sarebbe funzionale alla reimpostazione automatica delle parole-chiave riferite agli utenti, confrontando quelle di volta in volta pronunciate con il modello vocale ai medesimi riferito.

In proposito, le impronte vocali, unitamente ai dati da esse ricavati, costituiscono informazioni personali ai sensi dell´art. 4, comma 1, lett. *b*), del Codice con conseguente loro applicazione della disciplina in materia (*Provv*. 19 novembre 1999 [doc. *web* n. 42058] e *Provv*. 21 luglio 2005 [doc. *web* n. 1150679]; *v.* pure il documento di lavoro sulla biometria del Gruppo art. 29, Direttiva 95/46/Ce -WP80-, punto 3.1).

L´Autorità, ferma restando la necessità del consenso degli interessati (art. 23 del Codice; *cfr*. altresì Provv. 1° febbraio 2007, punto 3.3. [doc. *web* n. 1381983]; *Provv*. 26 luglio 2006, punto 3.3. [doc. *web* n. 1318582]; *Provv*. 15 giugno 2006, punto 3.2. [doc. *web* n. 1306523]) e la predisposizione di sistemi alternativi per la reimpostazione della *password*, ha comunque prescritto alcuni accorgimenti a garanzia degli utenti, con particolare riguardo alle istruzioni a disposizione degli utilizzatori del sistema, alle misure organizzative per prevenire rischi di impiego abusivo dei dati raccolti e alla cancellazione dei dati vocali dei lavoratori successivamente alla cessazione del rapporto di lavoro o di collaborazione (*Provv*. 28 febbraio 2008 [doc. *web* n. 1501094]).